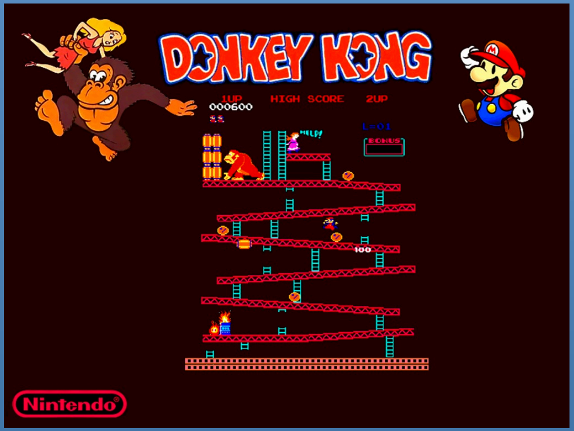
Video Games – From Spacewar! to Today

• Explosive rapid-fire space action • 1 or 2 players are challenged to destroy asteroids and enemy spacecraft • New Atari-designed QuadraScan™ display system • New personal high score table display • Optional "Hyperspace" • Optional coinage including Susan B. Anthony coin slot • Bonus play at 10,000 points.

The Japanese Invasion - Shigeru Miyamoto



id Software, Valve, and the Future

The Turing Test: A Timely Study

Adi Fuchs

COS583 Great Moments in Computing, Spring 2015

The Test Itself

- ❑ How does it reflect the progress in AI research?

- ❑ Does it say anything about consciousness?

- ❑ Does it say nothing at all, aside from human gullibility?

Passing the Turing Test

❑ Will it mark the rise of the machines?

❑ Is it even possible?

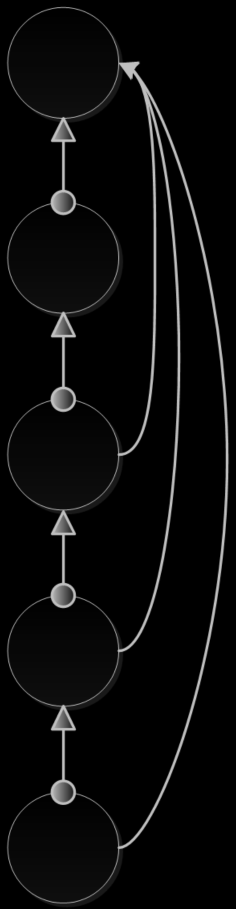
❑ How would we know if we did?

The Loebner Prize

- ❑ The annual “Imitation Game” Olympics, first held in 1991
- ❑ X terminals, at least 2 are human and 2 are computers
- ❑ Several judges, each talks to the terminal
- ❑ This year, 33% of the judges mistaken a machine to be human

Citation Chain

- ❑ Each cites its predecessor and the original paper
- ❑ 1950: “Can machines think?”
- ❑ 1991: “Let’s create a ‘practical Turing test’”
- ❑ 1992: “Practicing the Turing test makes no sense”
- ❑ 2000: “Maybe we should change the Turing test?”
- ❑ 2012: ”It’s time for the Turing test to go…”



Cryptography -> Bitcoin

Ben Stallworth

Bitcoin

- Distributed Electronic Currency
- Public Ledger of Transactions
- Peer to Peer System
- Currently Supporting Burgeoning Start-up Industry

How does Bitcoin relate to a great moment?

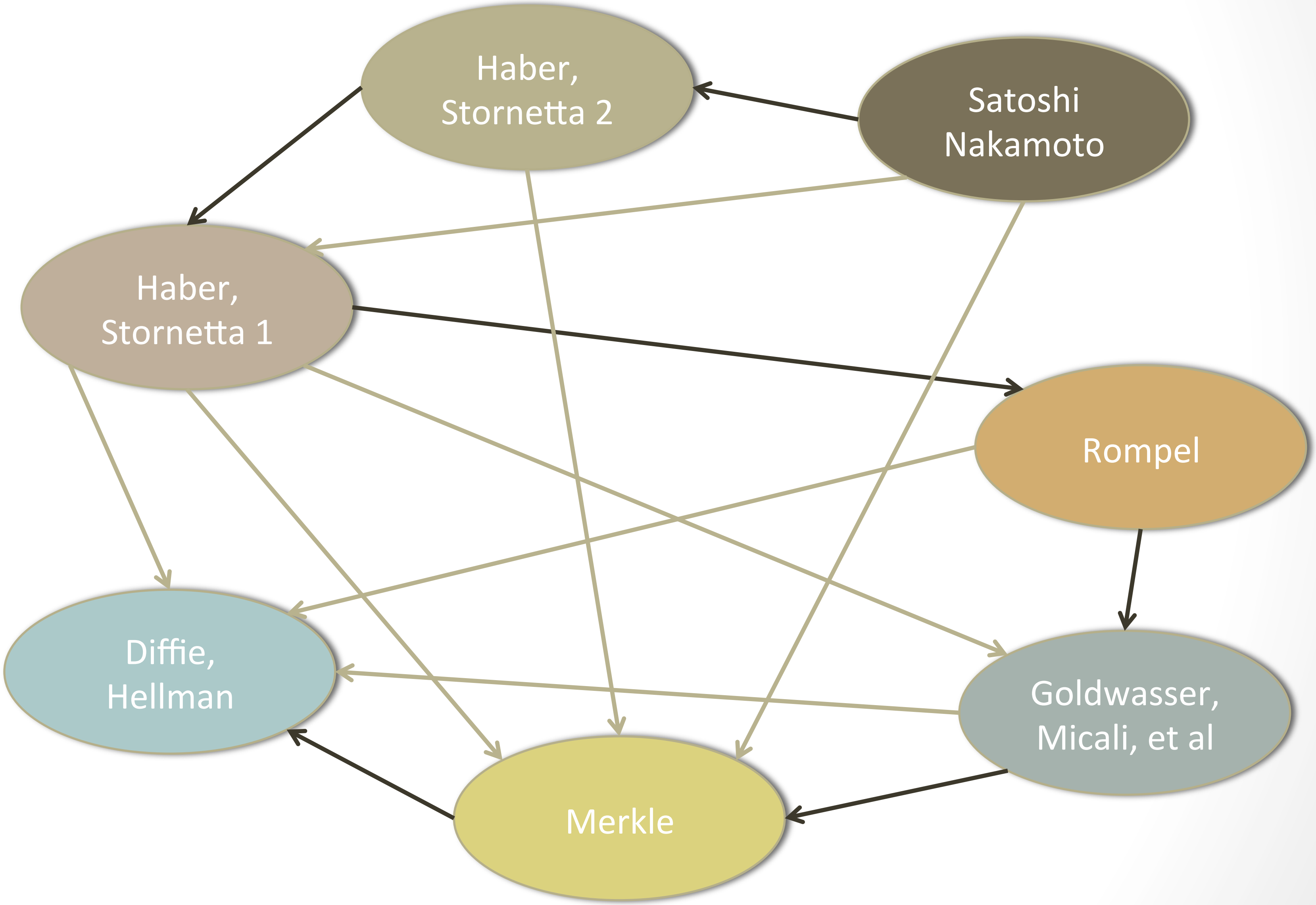
- Application of ideas/principles from Diffie-Hellman
  - Distributed System of Trust
  - Verifying Identity using Public/Private Keys
  - Hash and One-Way Functions
  - Secure Digital Signatures

- Ideas Developed
  - Implementation of Digital Signatures
  - Hash Functions from One-Way Functions
  - Time Stamping and Identity Verification

Papers (in Citation Order)

- Diffie-Hellman. “New directions in cryptography”
- Merkle. “Secrecy, Authentication, and Public Key Systems”
- Goldwasser, Micali, et al. “A Secure Digital Signature Scheme”
- Rompel. “OWF are Necessary and Sufficient for Secure Signatures”
- Haber, Stornetta. “How to Time-Stamp a Digital Document”
- Haber, Stornetta. “Secure Names for BitStrings”
- Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”

Citation Web



The Internet to Distributed Data

How Locating Objects in a Network Has Evolved

Cody Wilson
COS 583
Prof. Martonosi
April 27th, 2015

Step 1: Protocols

- Cerf and Kahn[1] → RFC 791: Internet Protocol[5]
- RFC 791 → RFC 1256: ICMP Router Discovery Messages[2]
    - Router Solicitations and Advertisements
    - ICMP on top of IP
- RFC 1256 → Locating nearby copies of replicated Internet servers[3]
    - Anycast
    - Routing Probes - traceroute
    - Triangulated distance metrics

Step 2: Data Structures

- Nearby Copies of Servers → Nearby Copies of Replicated Objects[4]
  - From a central server of distances to tree of objects on each node
- Nearby Copies of Replicated Objects → Chord Distributed Hash Table[6]
  - From a tree of objects on each node, to a tree of nodes to find objects
  - Scalability

References

[1] V. G. Cerf and R. E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Transactions on Communications,* vol. Com-22, May 1974, 1974.

[2] S. Deering, "RFC: 1256: ICMP router discovery messages," September 1991, 1991.

[3] J. D. Guyton and M. F. Schwartz, *Locating Nearby Copies of Replicated Internet Servers.* ACM, 1995.

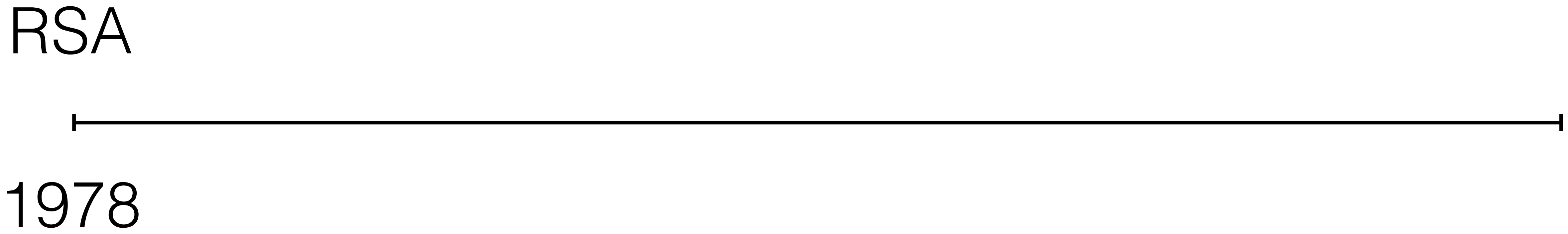
[4] C. G. Plaxton, R. Rajaraman and A. W. Richa, "Accessing nearby copies of replicated objects in a distributed environment," *Theory of Computing Systems,* vol. 32, pp. 241-280, 1999.

[5] J. Postel, "RFC 791: Internet protocol," 1981.

[6] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review,* vol. 31, pp. 149-160, 2001.

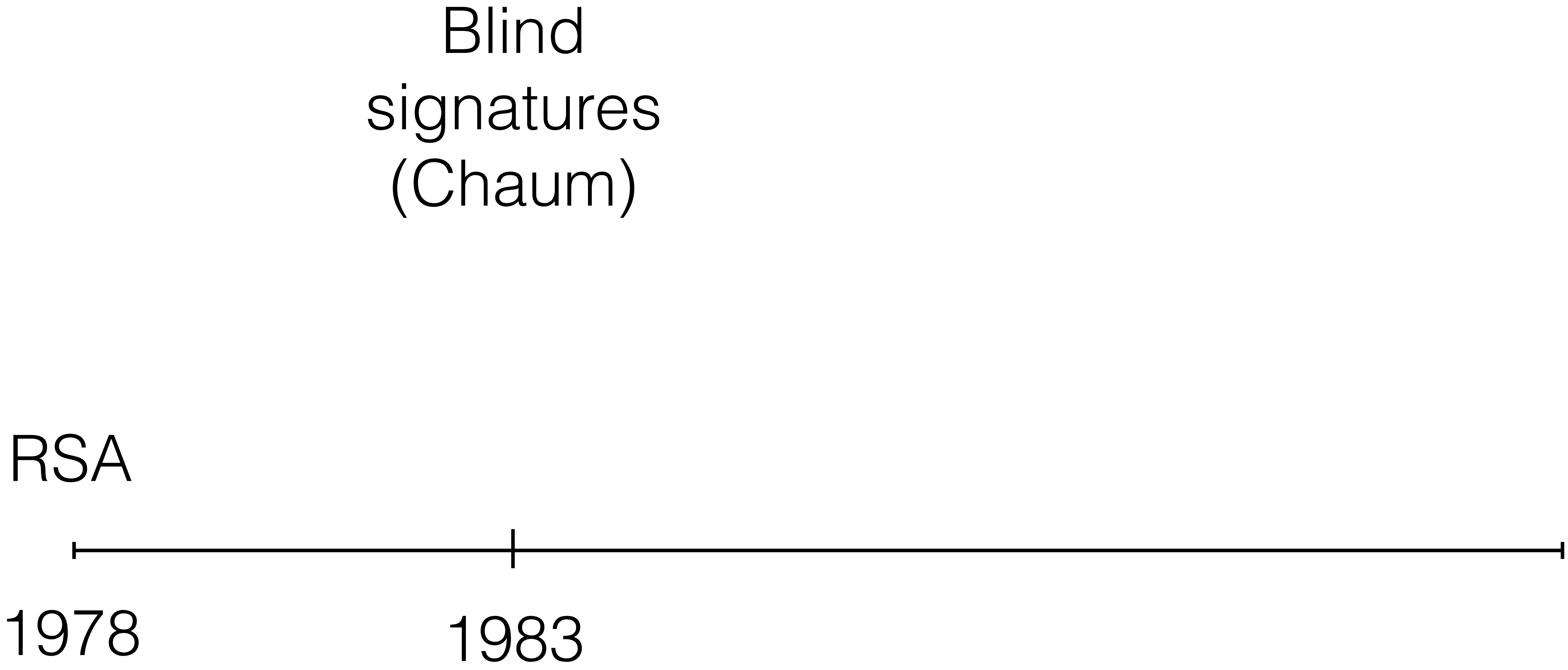
A Historical Tour of RSA Vulnerabilities

James Evans & Charles Marsh
COS 583
Spring 2015



RSA

1978

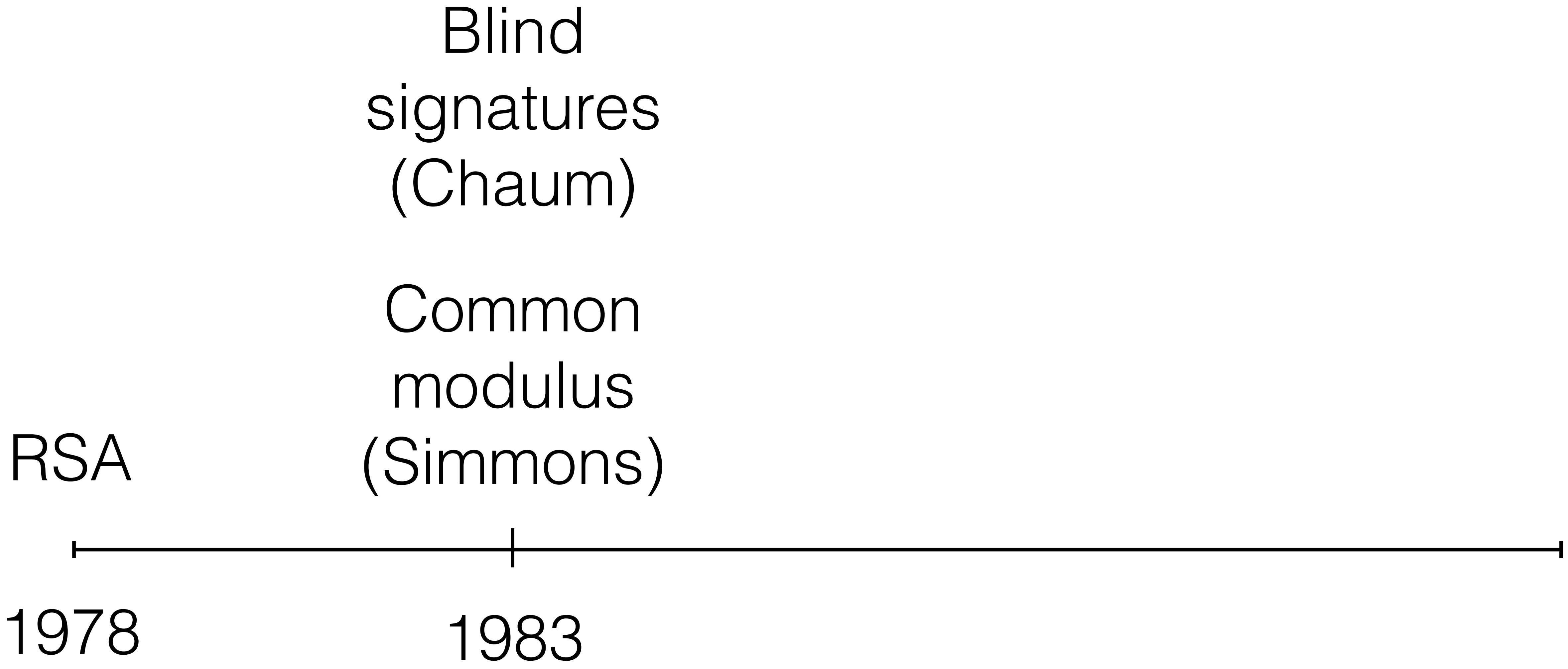


Blind signatures (Chaum)

RSA

1978

1983



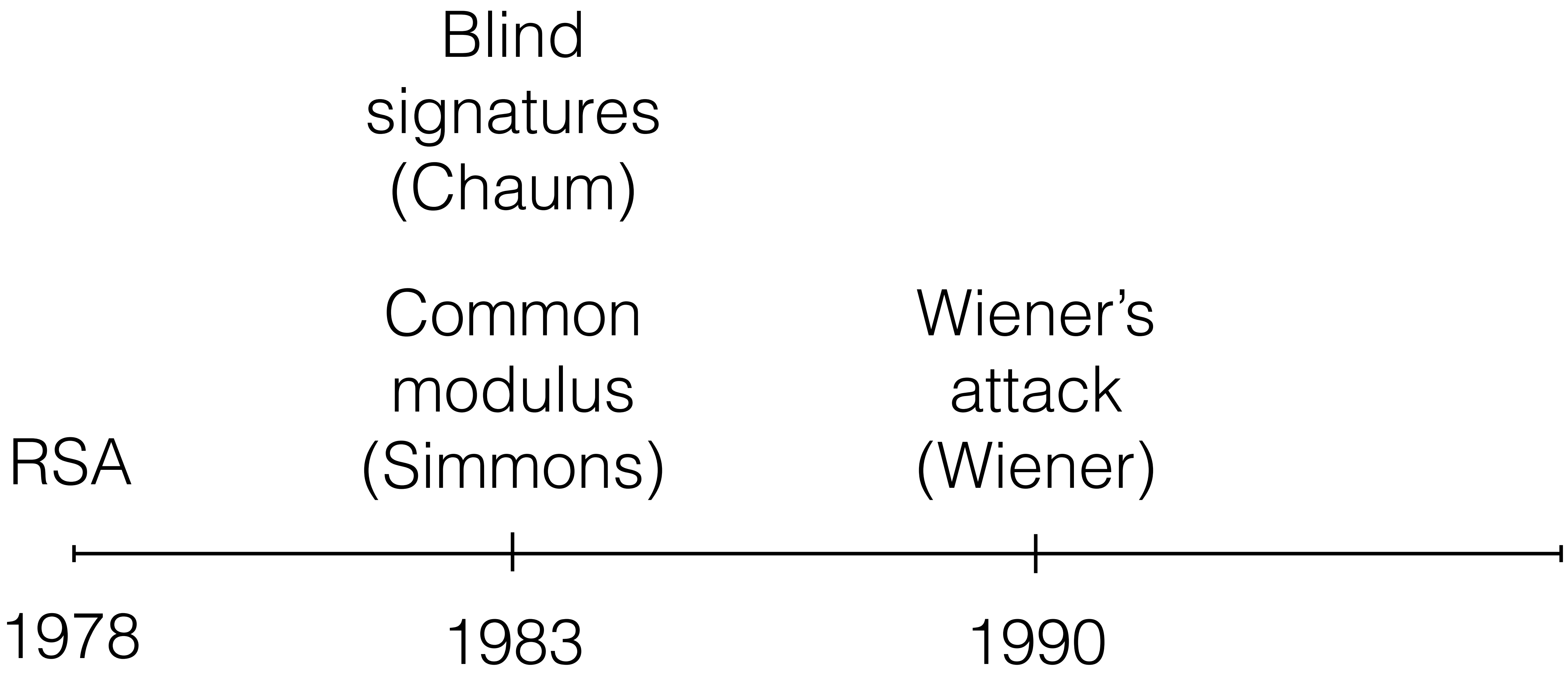
Blind signatures (Chaum)

Common modulus (Simmons)

RSA

1978

1983



Blind
signatures
(Chaum)

Common
modulus
(Simmons)

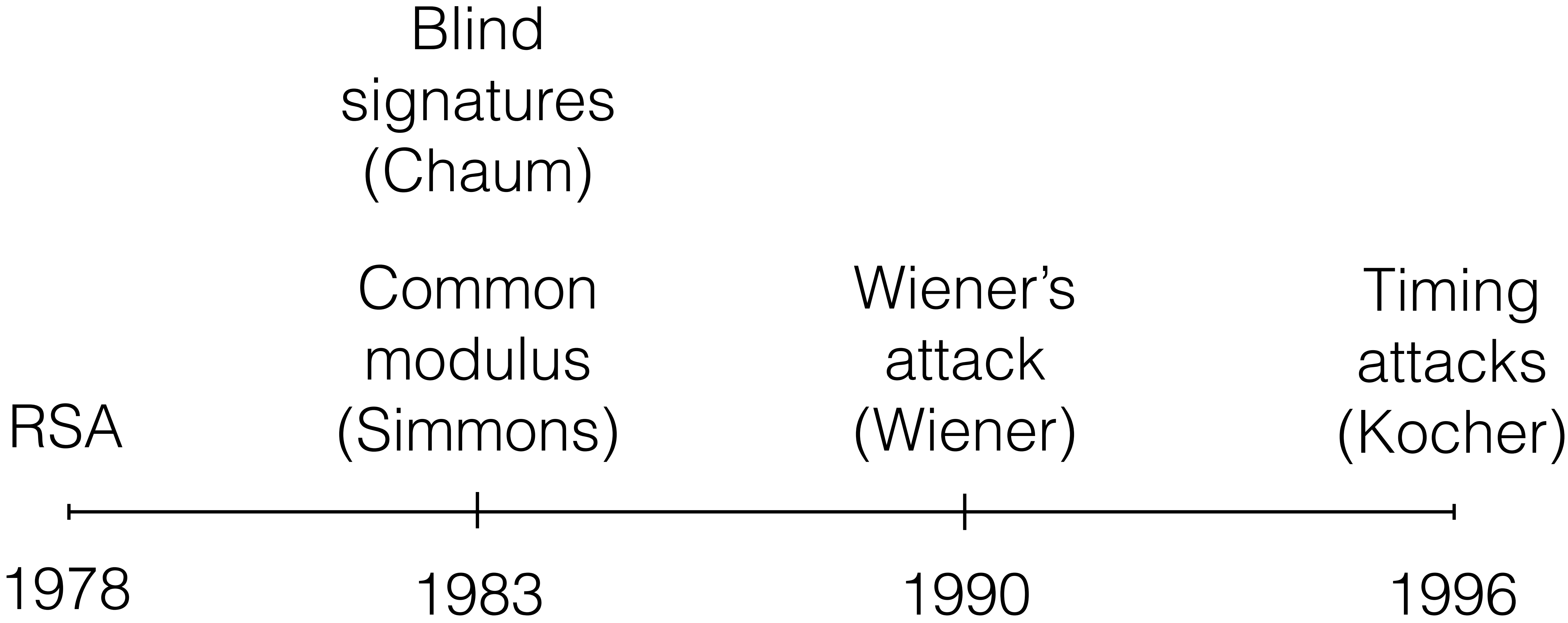
Wiener's
attack
(Wiener)

RSA

1978

1983

1990



RSA

1978

Blind signatures (Chaum)

Common modulus (Simmons)

1983

Wiener's attack (Wiener)

1990

Timing attacks (Kocher)

1996

Capture the Flag (CTF)

The Backstory

On January 3rd, 1978, a large bank lost $100 million when a hacker broke into its database. Based on a tip, the FBI has investigated a cryptography researcher by the name of **Bob Badguy** for the crime, but they haven't managed to find much evidence in the 37 years since. **Badguy is known to have had a keen interest in the emerging field of public-key cryptography**, and covered his tracks using the cutting-edge cryptography available every step of the way for the past four decades.

Capture the Flag (CTF)

1. Deterministic attack: find Badguy’s password
2. Common modulus attack: decrypt identical messages to accomplices
3. Iterated encryption: decrypt his wire transfer metadata
4. …

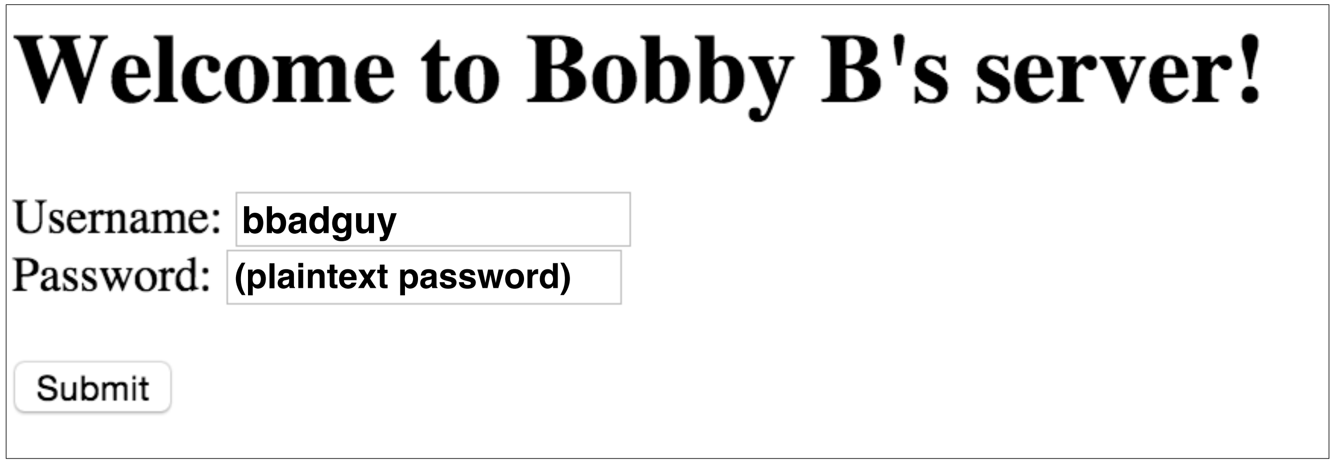
Capture the Flag (CTF)

1. Deterministic attack: find Badguy’s password
2. Common modulus attack: decrypt identical messages to accomplices
3. Iterated encryption: decrypt his wire transfer metadata
4. …

Goals

- Learn about the academic history of RSA
- Learn about vulnerabilities in the protocol
- Create an educational tool for others

RSA-Encrypted password:
9839834209234


Welcome to Bobby B's server!

Username: bbadguy
Password: (plaintext password)

Translation in the Face of Varying Memory Consistency Models

Caroline Trippel

Project Status Lightening Round

04.27.2015

The first MCM: Sequential Consistency

- MCMs specify the allowed behavior of a multithreaded program executing with shared memory [Sorin et al., 2011].

- First defined by [Lamport 1979], execution is the same as if:

  (R1) Memory operations of each individual processor appear in program order (PO)

  (R2) Memory operations of all the processors were executed in some global sequential order

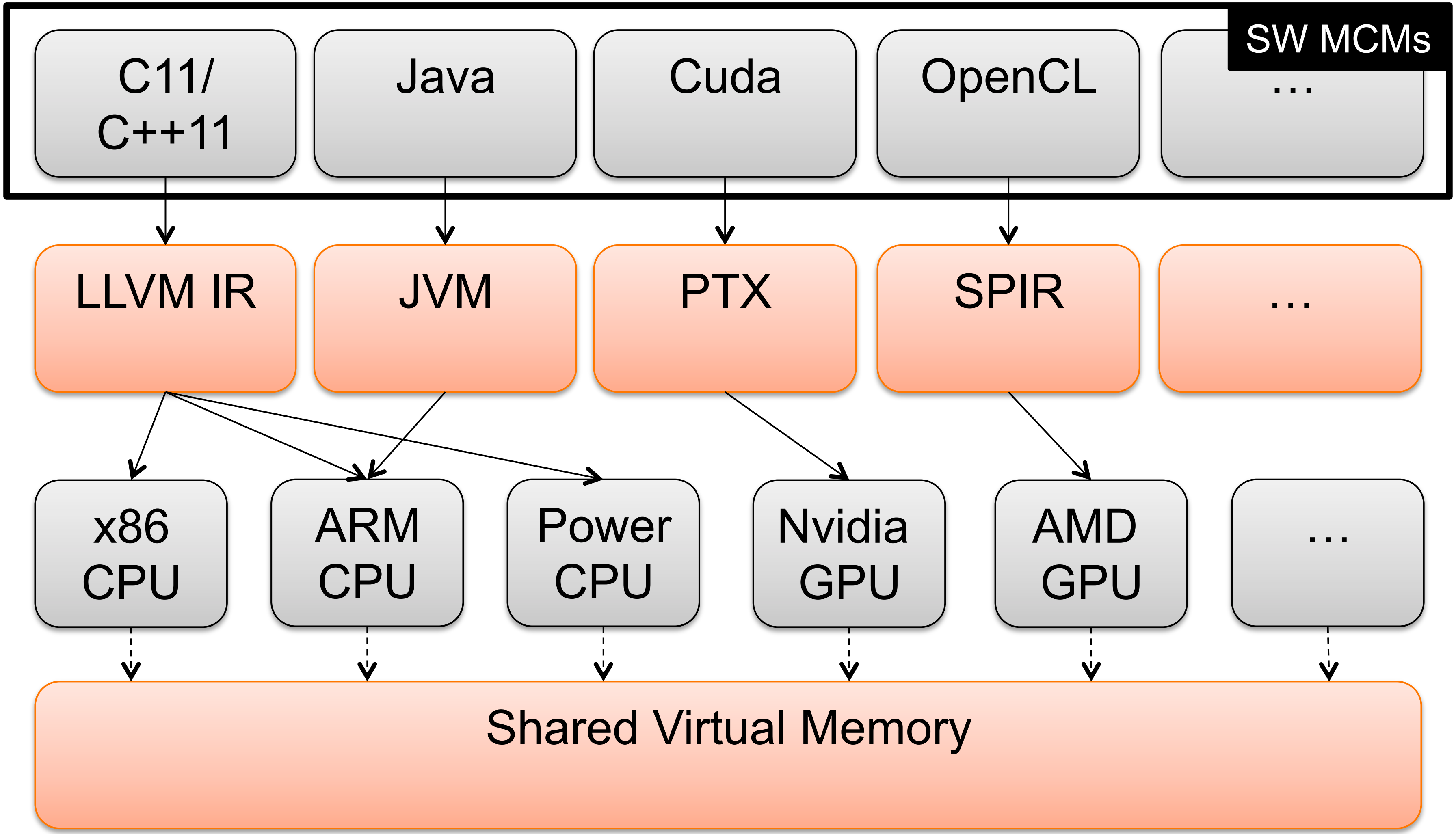
Program

Thread 0	Thread 1
x=1	r1=y
y=1	r2=x

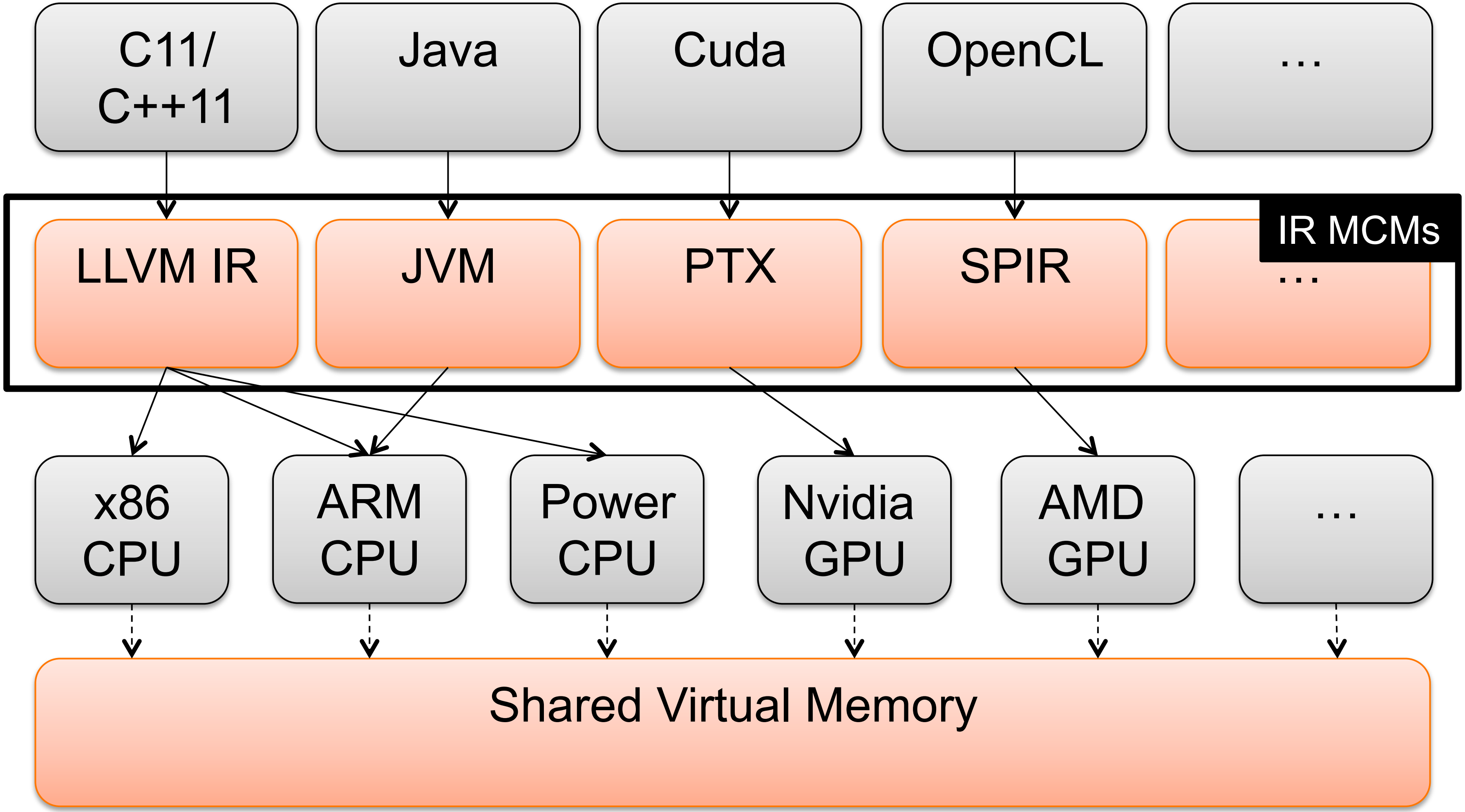
Legal Executions

x=1	x=1	x=1	r1=y	r1=y	r1=y
y=1	r1=y	r1=y	r2=x	x=1	x=1
r1=y	y=1	r2=x	x=1	r2=x	y=1
r2=x	r2=x	y=1	y=1	y=1	r2=x

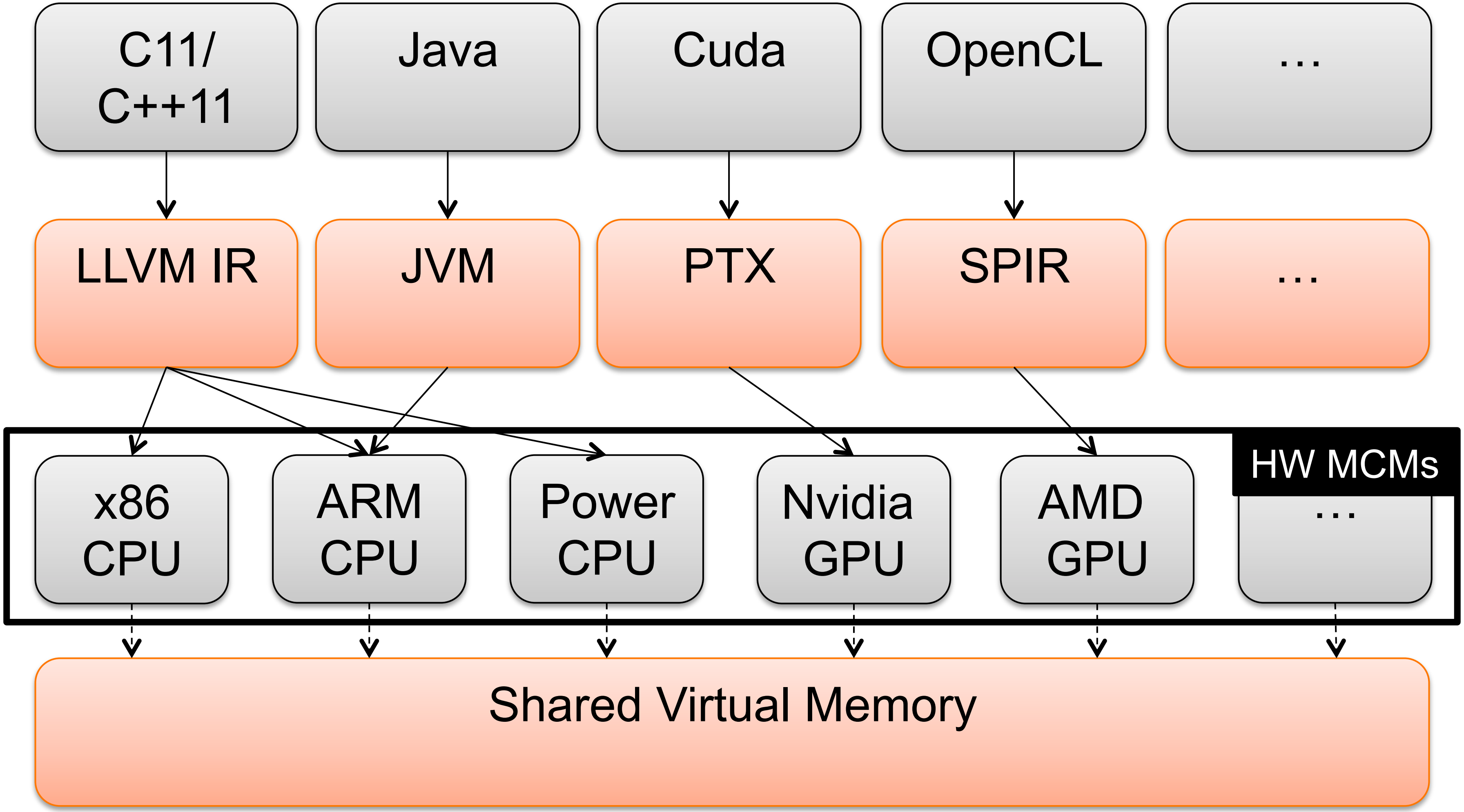
Memory Consistency Models



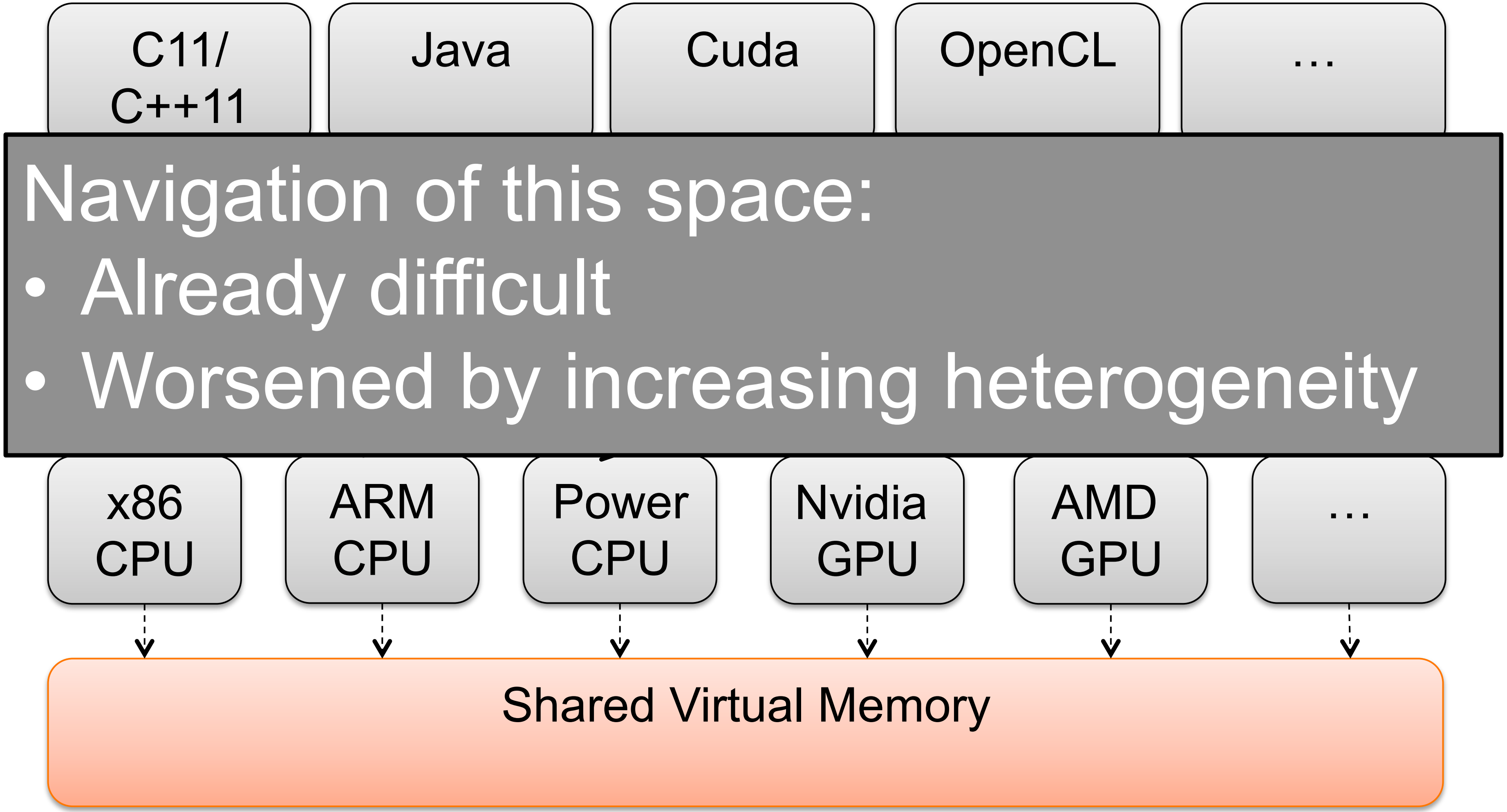
Memory Consistency Models



Memory Consistency Models



Memory Consistency Models



C11/ C++11

Java

Cuda

OpenCL

…

Navigation of this space:

- Already difficult
- Worsened by increasing heterogeneity

x86 CPU

ARM CPU

Power CPU

Nvidia GPU

AMD GPU

…

Shared Virtual Memory

ArMOR Framework

1. The ArMOR syntax [Lustig et al., 2015]
   - Framework for specifying, comparing, and translating between memory consistency models.
   - Architecture-independent yet precise format for specifying the semantics of memory ordering requirements (MORs).
2. Dynamic translation with ArMOR [Lustig et al., 2015]
3. Install-time static translation with ArMOR

ArMOR ISA-Assisted Optimizations

- What if we had access to compiler metadata?
- **Thread private accesses**
  - Relatively straightforward compiler analysis can classify as many as 81% of memory accesses [Singh et al., 2012] as thread-private
  - We found that an average of 75% of memory accesses were stack accesses
- **Data-race-free code**
  - C++ execution guaranteed to be SC for non-DRF programs, else **no** semantics are given [Boehm and Adve, 2008]
  - Parsec benchmark suite written in C++

SKETCHPAD

IN JAVA

David Fridovich-Keil
ELE 583, Princeton University

No arcs, but...

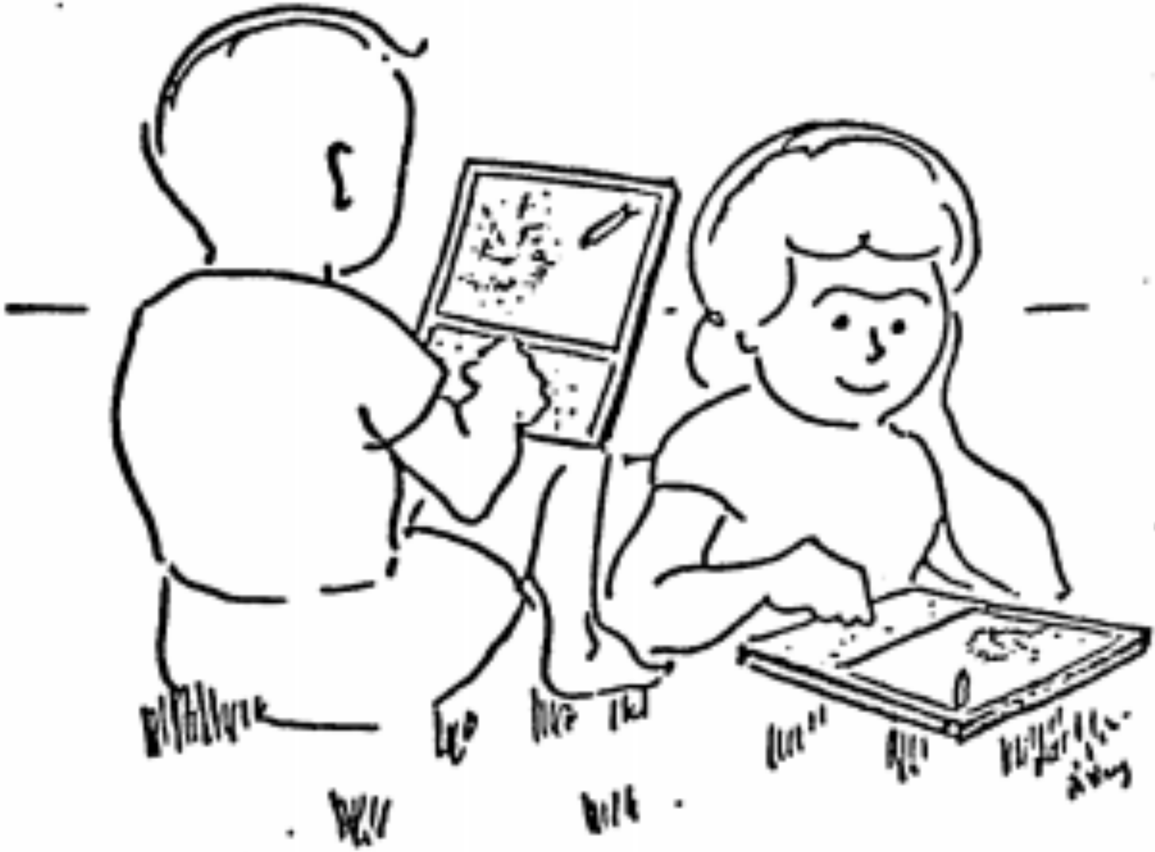
- Point, line, composite shapes
- Point and line constraints
- Graph-based constraint satisifiability tester
- General, home-made nonlinear optimization for constraint satisfaction

Demo

http://youtu.be/GPbVSHIHLAY

Spacewar!

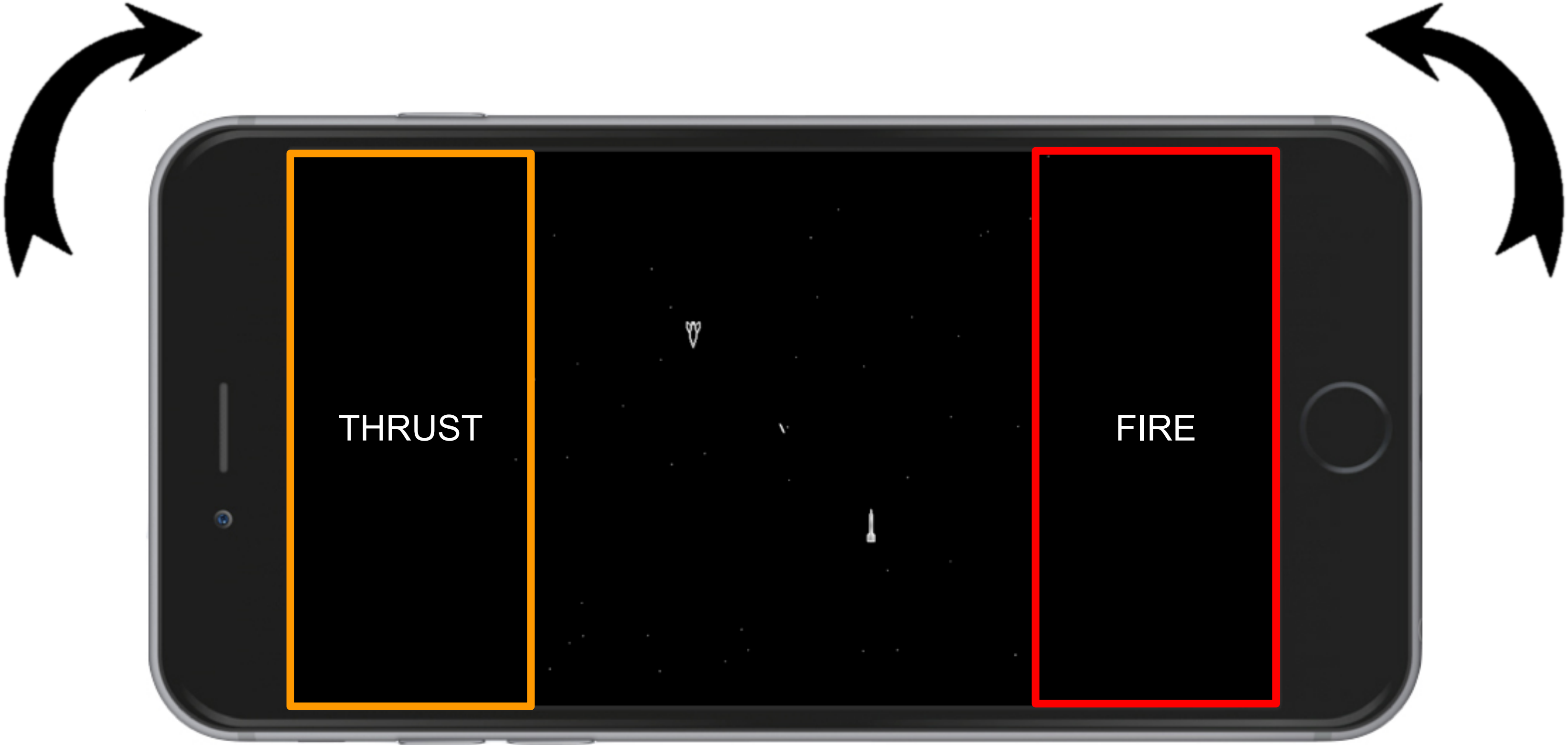
Dan Kang



Zap! With a beautiful flash and appropriate noise, Jimmy’s spaceship disintegrated; Beth had won Spacewar again. The nine-year-olds were lying on the grass of a park near their home, their DynaBooks hooked together to allow each of them a viewscreen into the space world where Beth's ship was now floating triumphantly alone.

Zap! With a beautiful flash and appropriate noise, Jimmy’s spaceship disintegrated; Beth had won Spacewar again. The nine-year-olds were lying on the grass of a park near their home, their DynaBooks hooked together to allow each of them a viewscreen into the space world where Beth's ship was now floating triumphantly alone.

Zap! With a beautiful flash and appropriate noise, Jimmy’s spaceship disintegrated; Beth had won Spacewar again. The nine-year-olds were lying on the grass of a park near their home, their iPhones hooked together to allow each of them a viewscreen into the space world where Beth's ship was now floating triumphantly alone.


THRUST
FIRE

Current Progress

- The ship can turn!
- The ship can thrust!
- The ship can fire!
- The ship is lonely...

Future Work

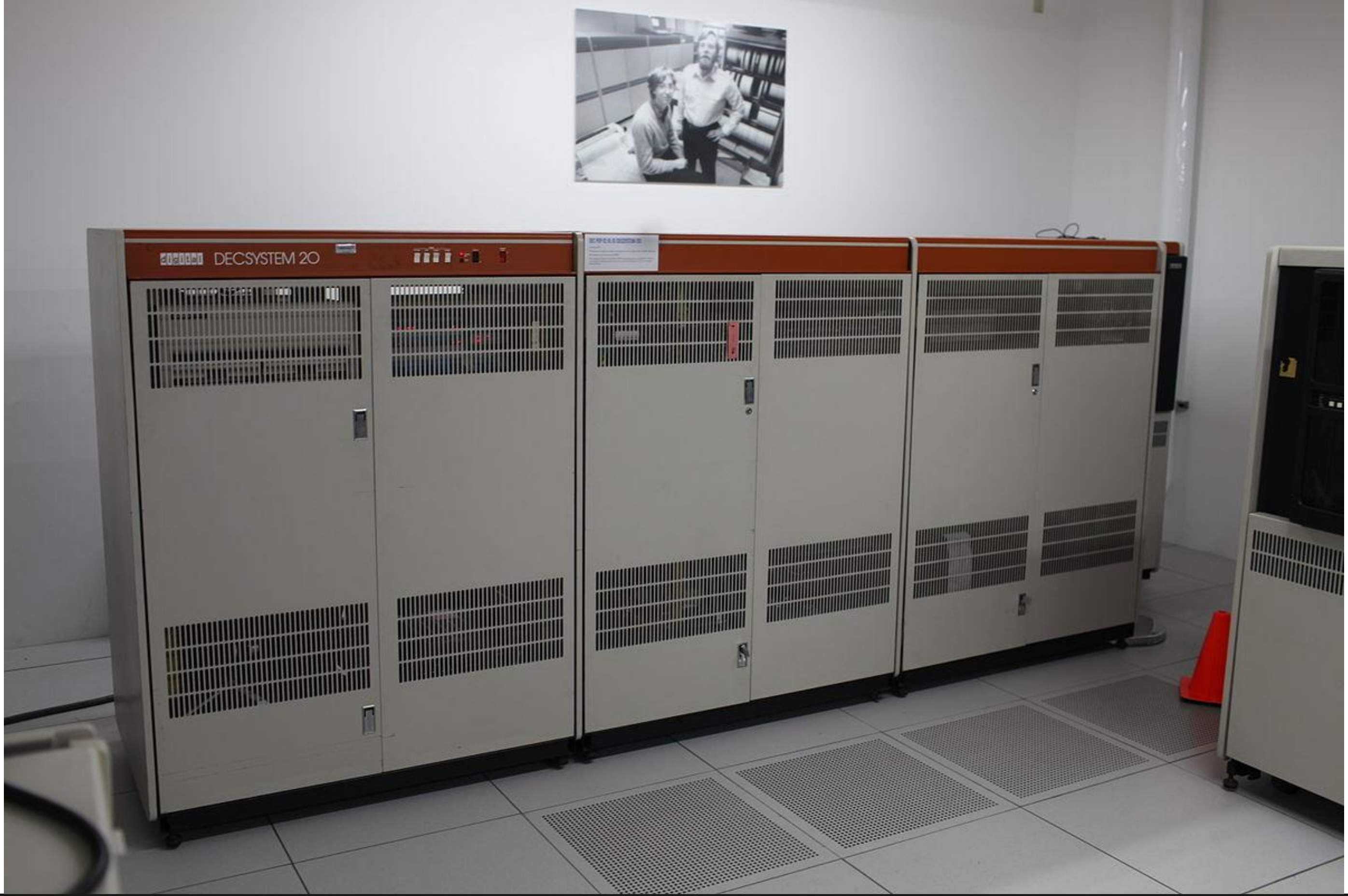
- Multiplayer!
- A star!
- Collisions and explosions!

CGL@LCS

Erica Portnoy

"Living Computer Museum pano 01" by Joe Mabel. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Living_Computer_Museum_pano_01.jpg#/media/File:Living_Computer_Museum_pano_01.jpg

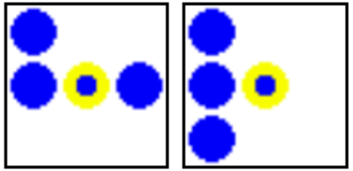
DEC VAX-11/780-5: VMS



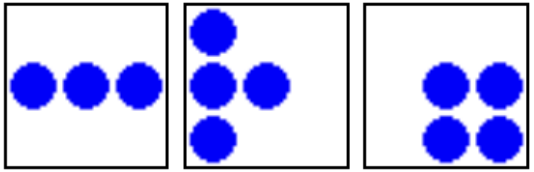
DEC PDP-10: KL-10 (DECSYSTEM-20)

Conway’s Game of Life (http://www.math.com/students/wonders/life/life.html)

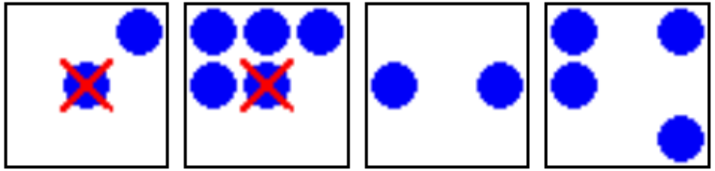
- A dead cell with exactly three live neighbors becomes a live cell (birth).



- A live cell with two or three live neighbors stays alive (survival).

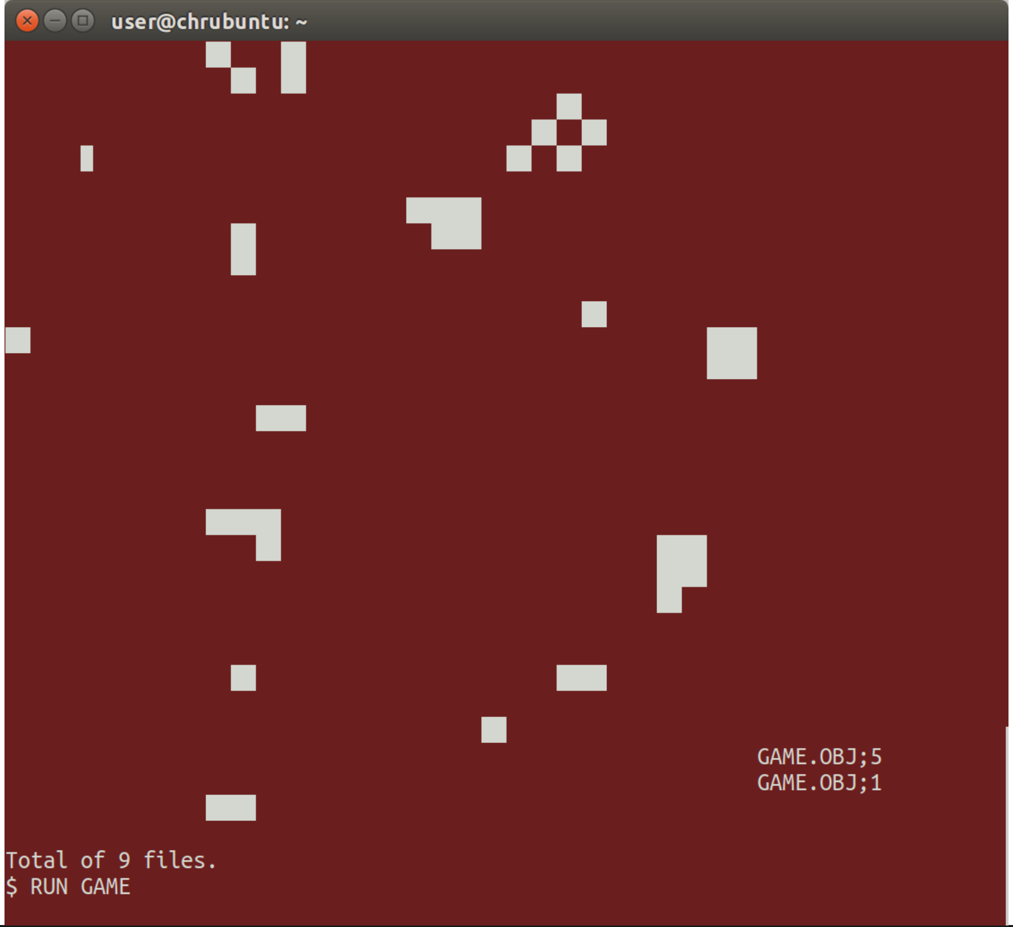


- In all other cases, a cell dies or remains dead (overcrowding or loneliness).



Virtual Memory

- 1961: Kilburn/Atlas
- 1967: MULTICS
- 1977: VAX minicomputer



```
GAME.OBJ;5
GAME.OBJ;1

Total of 9 files.
$ RUN GAME
```

So far

TODO

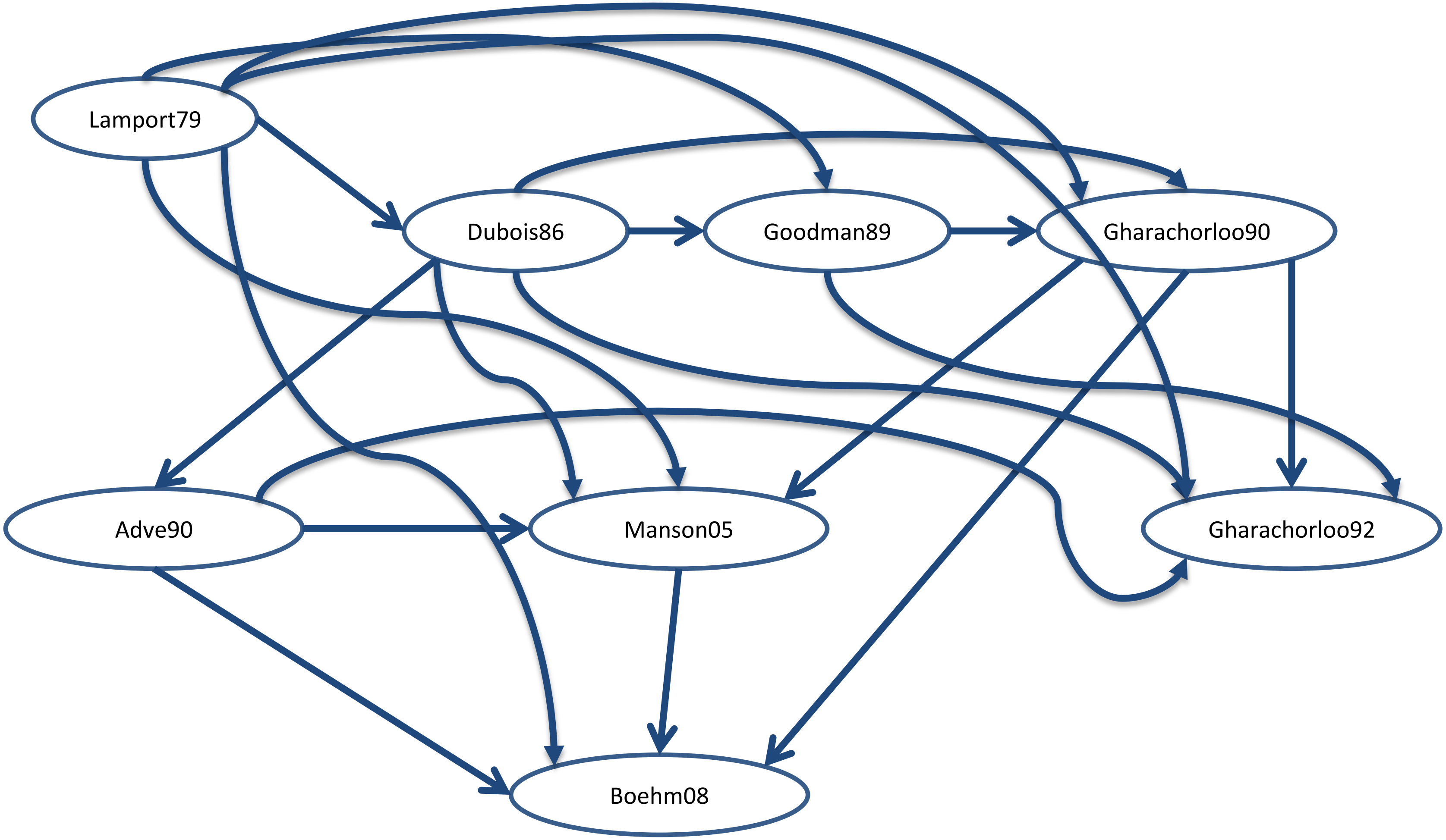
- Improve animation
- PDP-10

http://www.cs.princeton.edu/~jfrankle/sketchpad/sketchpad.html

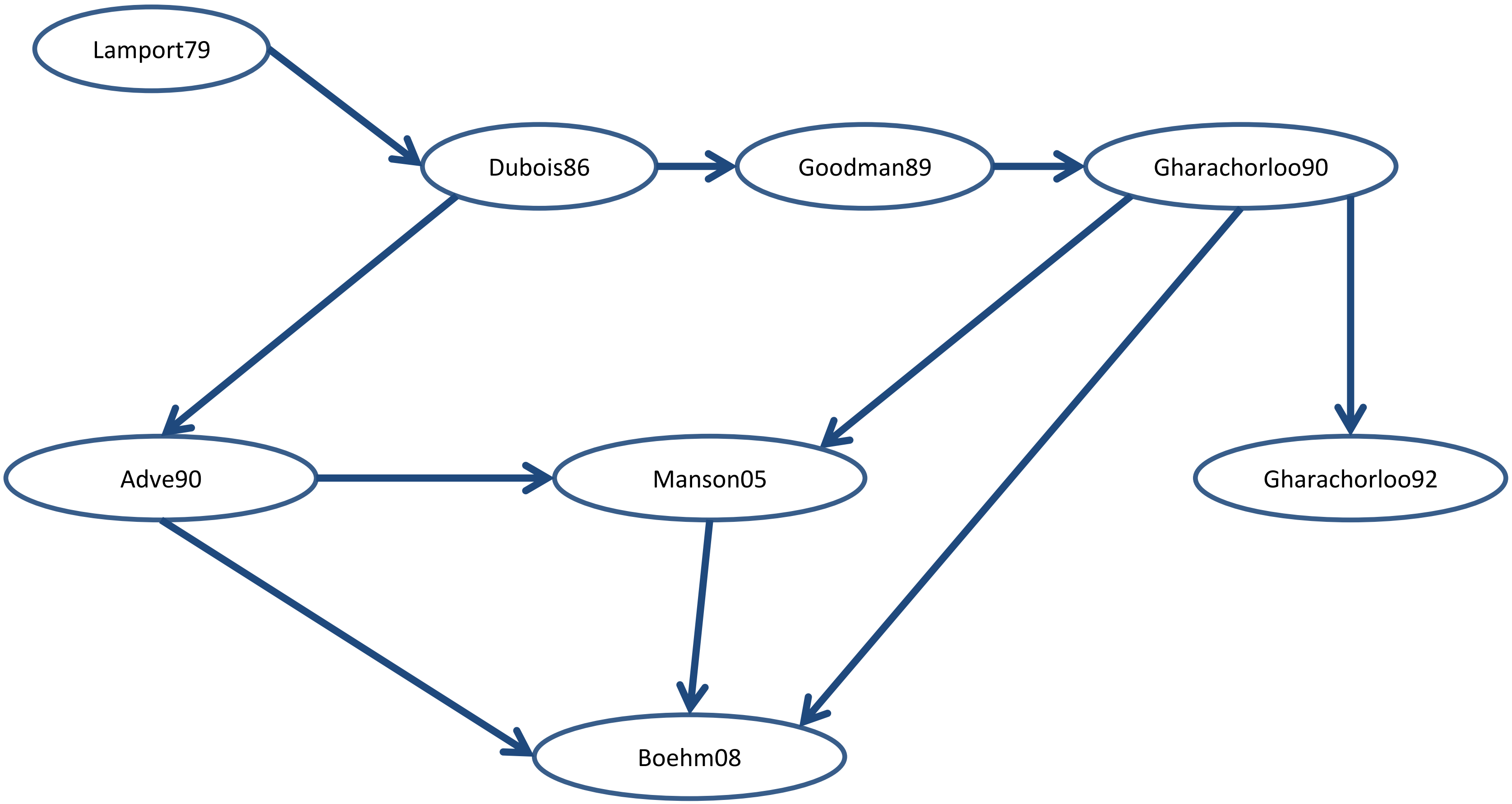
Citation Chain from Lamport's Sequential Consistency Paper

Yatin Manerkar

Citation Chain (All Links)

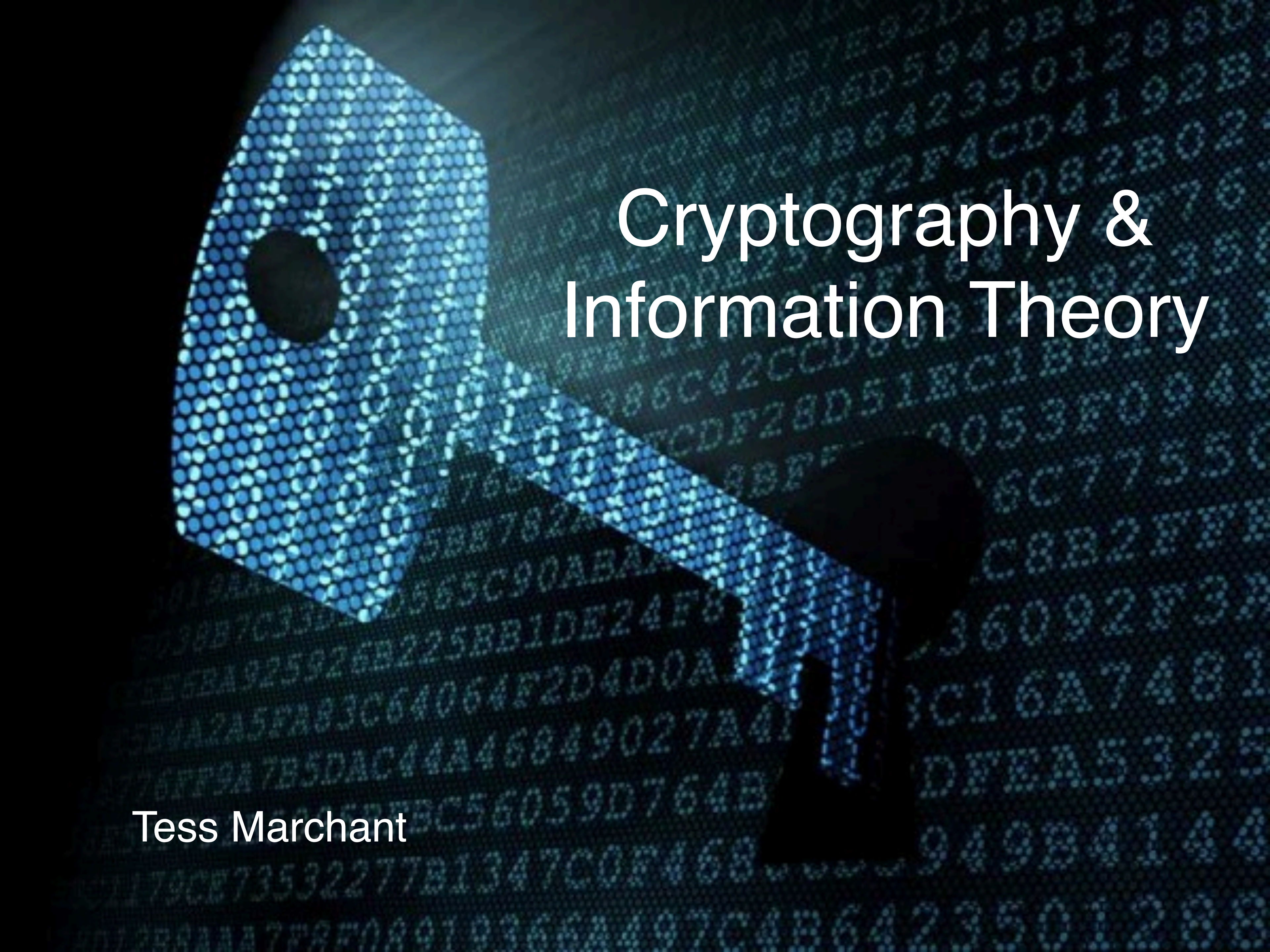


Citation Chain (Major Links)



Work Completed and Work Remaining

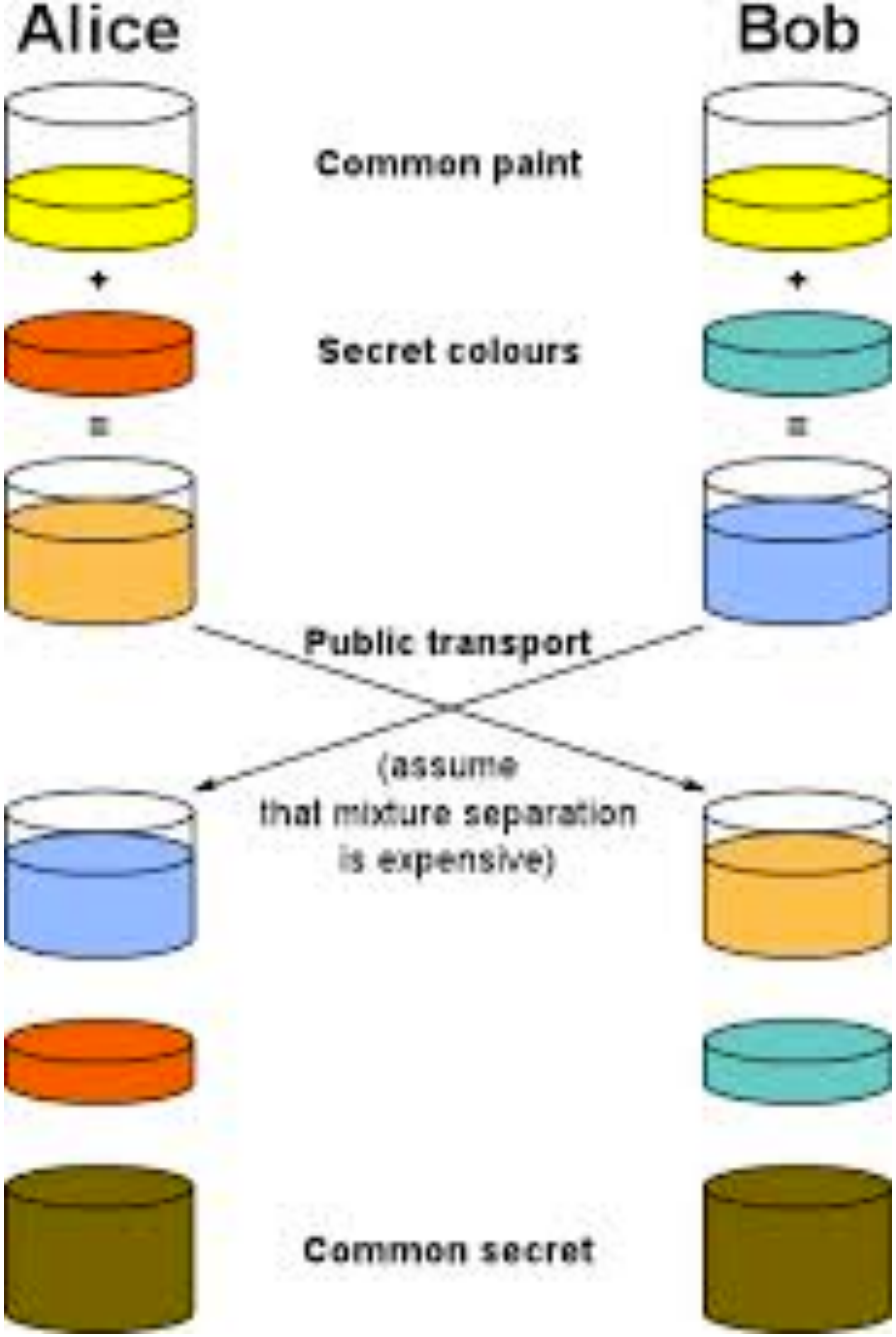
- Have read through papers to understand major steps forward at each point in the chain
- Need to re-read to understand the smaller and more subtle improvements between papers



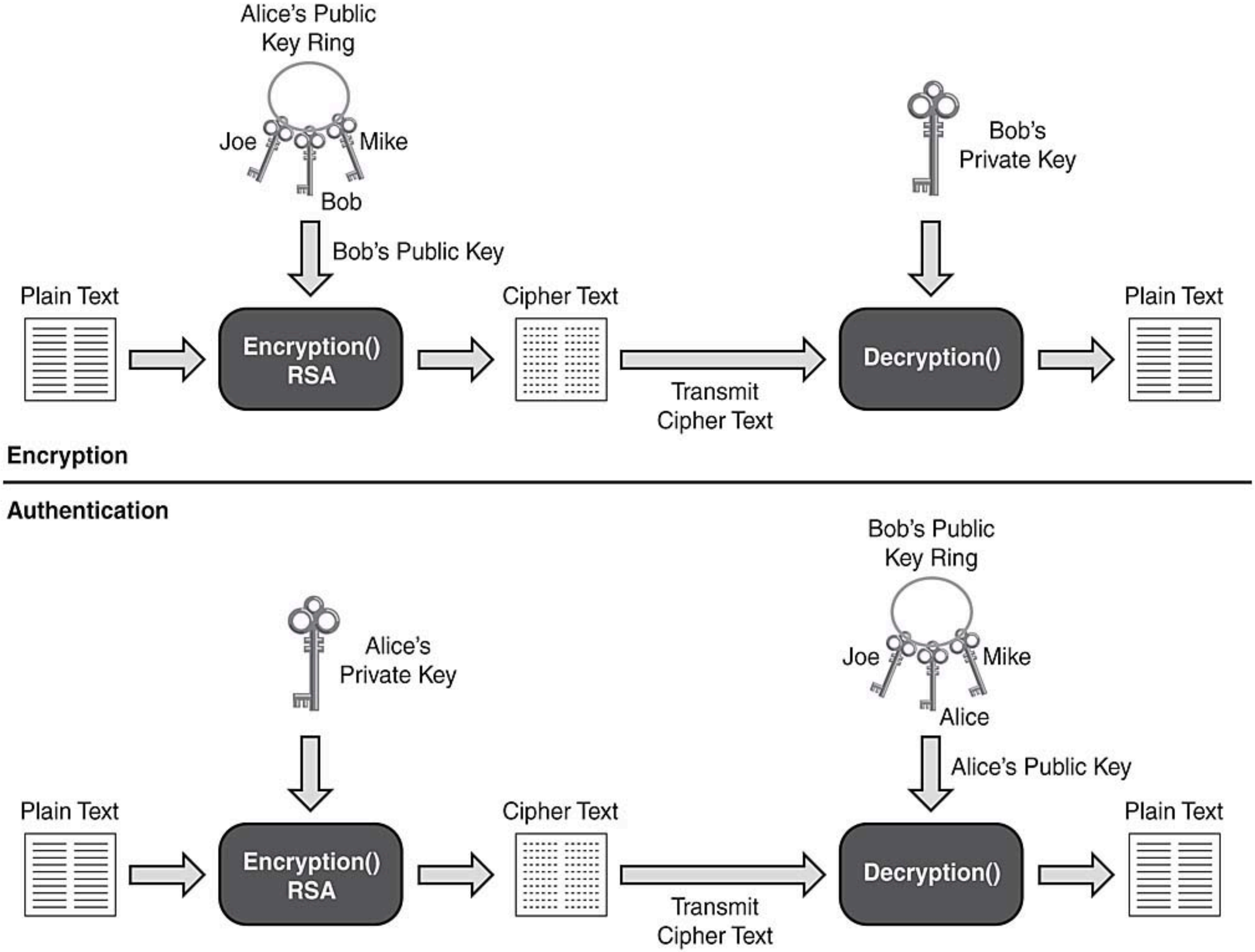
Cryptography & Information Theory

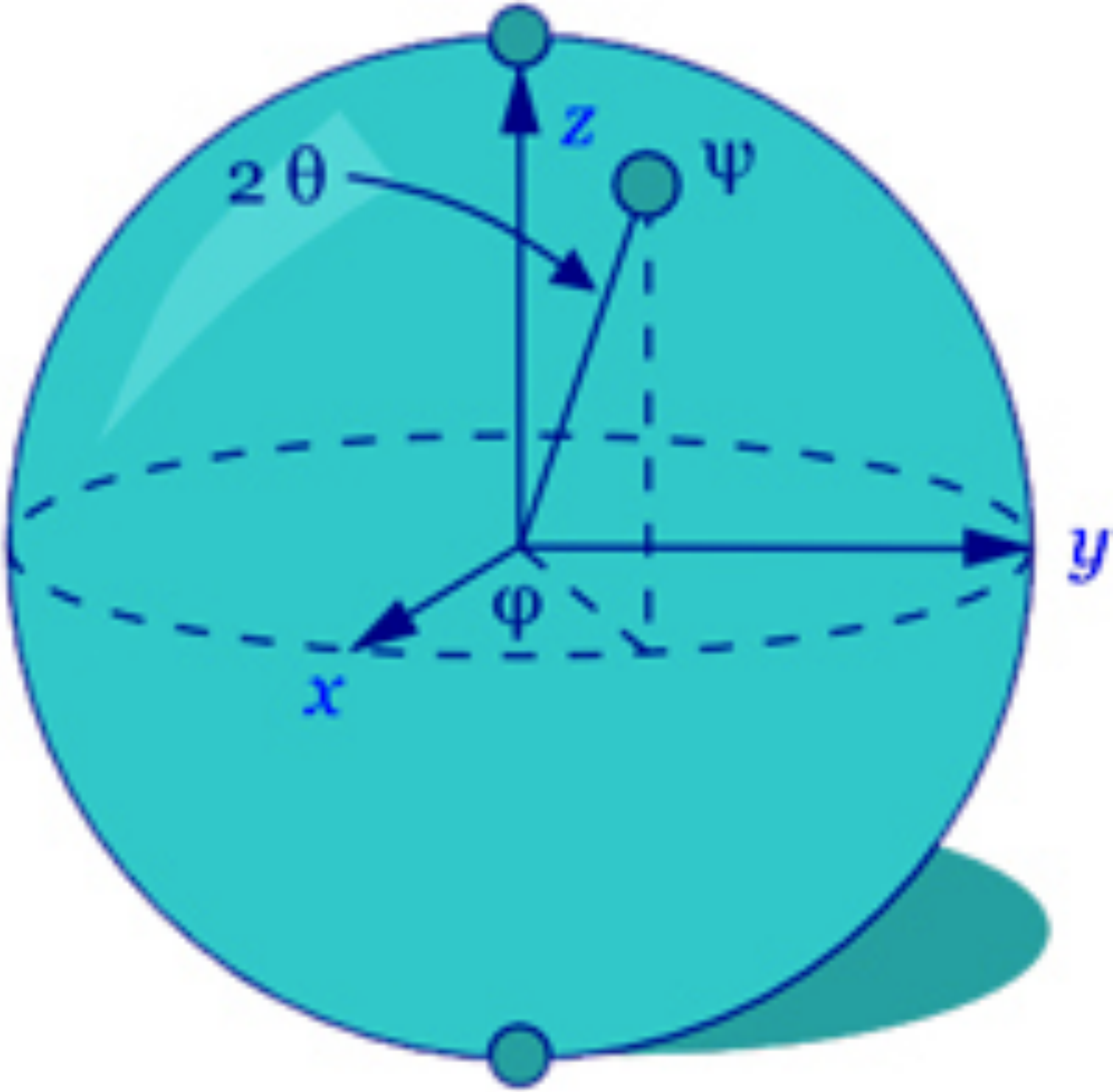
Tess Marchant

MERKLE



DIFFIE-HELLMAN


Alice's Public Key Ring
Joe
Mike
Bob
Bob's Public Key
Bob's Private Key
Plain Text
Encryption() RSA
Cipher Text
Transmit Cipher Text
Decryption()
Plain Text
Encryption
Authentication
Bob's Public Key Ring
Alice's Private Key
Joe
Mike
Alice
Alice's Public Key
Plain Text
Encryption() RSA
Cipher Text
Transmit Cipher Text
Decryption()
Plain Text


z
2 θ
Ψ
y
φ
x

“[Communication theory and cryptography] were so close you could not separate them.”

– Claude Shannon

- Introduction
  - Importance of crypto alongside all information theory
- Communication Theory of Secrecy Systems
  - Shannon’s one-time pads
  - Reference intro
- Protocols for public-key cryptosystems & New Directions in Cryptography
  - Explain need for public-key cryptosystems/infeasibility of one-time pads in the modern world
  - Use paint metaphor to explain public-key system
  - Relate to information theory/ scaling
- A Method for Obtaining Digital Signatures and Public-Key Cryptosystems & How to share a secret
  - Relate to MDH through the need for authentication alongside encryption
  - Explain the RSA algorithm
  - Relate to intro through need to trust people/entities that you share information with
- Quantum Cryptography
  - Describe findings in the paper
  - Explain how Quantum could disrupt RSA, and what can be done to counteract it
- Conclusion
  - Reiterate development of crypto
  - Reiterate relationship between IT and crypto

MapReduce’s Parallel Database Origins

Nevin Li

Background

- MapReduce – Programming model and implementation for processing large data sets in a parallel and distributed fashion on a cluster.
    - Map inputs into a list of pairs grouped by key, Reduce all pairs with the same key in some fashion.
- Meant to be read in conjunction with PageRank, but cut due to time constraints.
- David DeWitt blog post criticizing MapReduce for not being novel and using techniques the distributed database community have been using for a long time.

Paper Breakdown (Part 1)

- Application of Hash To Database Machine … (1983)
  - Hashing tuples by key into same buckets to optimize joins.
- Multiprocessor Hash-Based Join Algorithms (1985)
  - Optimizations made to such hash algorithms.
- The Case for Shared Nothing Architecture (1986)
  - Multiprocessor systems should not share memory or disk.

Paper Breakdown (Part 2)

- Prototyping Bubba, A Highly Parallel Database System (1990)
  - Early parallel database prototype featuring the hash-based join algorithms.
- High-Performance Sorting on Networks of Workstations (1997)
  - MapReduce-like backend involving source workers partitioning the data to be sorted and sent to reduce workers.

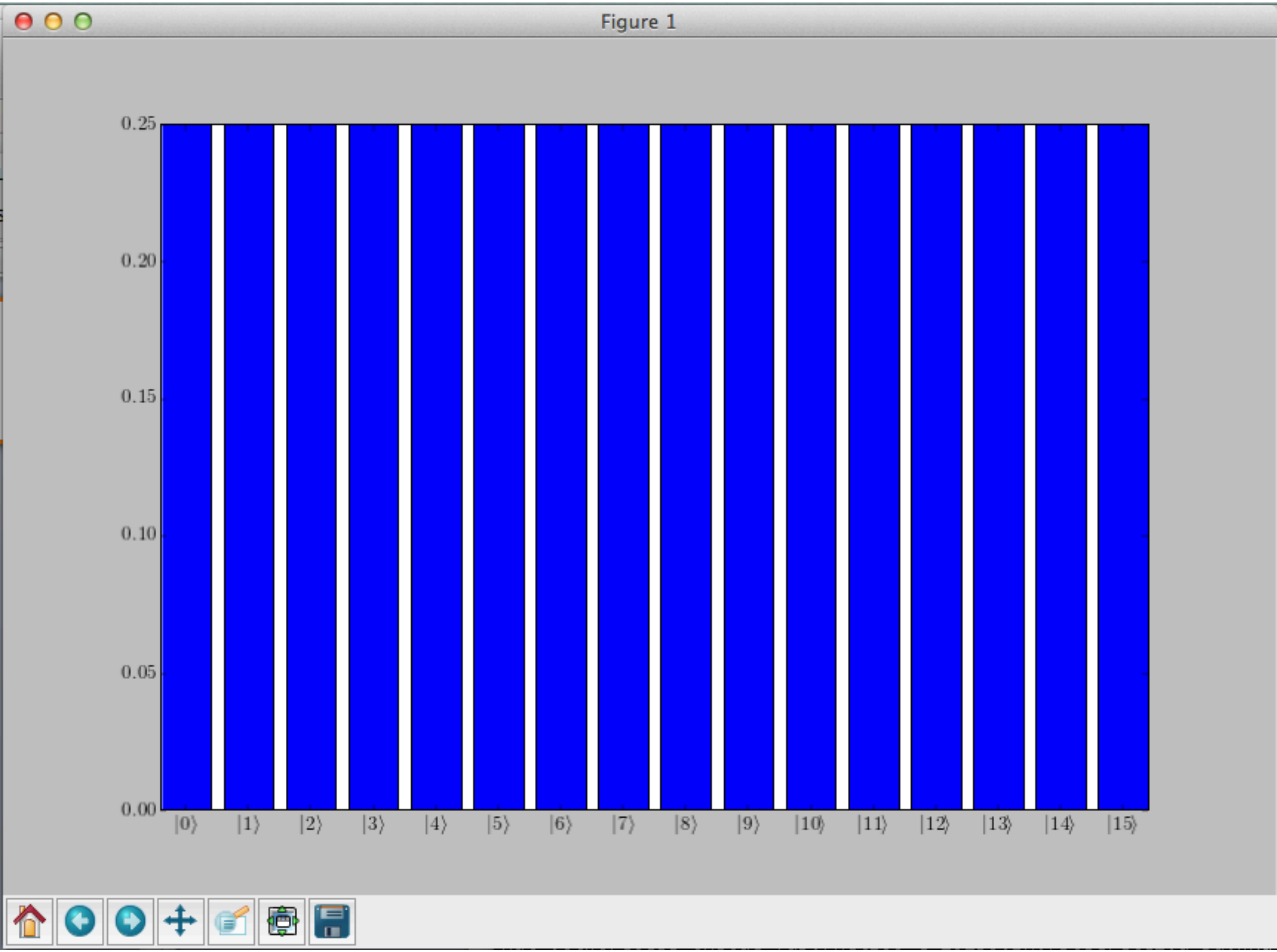


Figure 1
0.25
0.20
0.15
0.10
0.05
0.00
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩

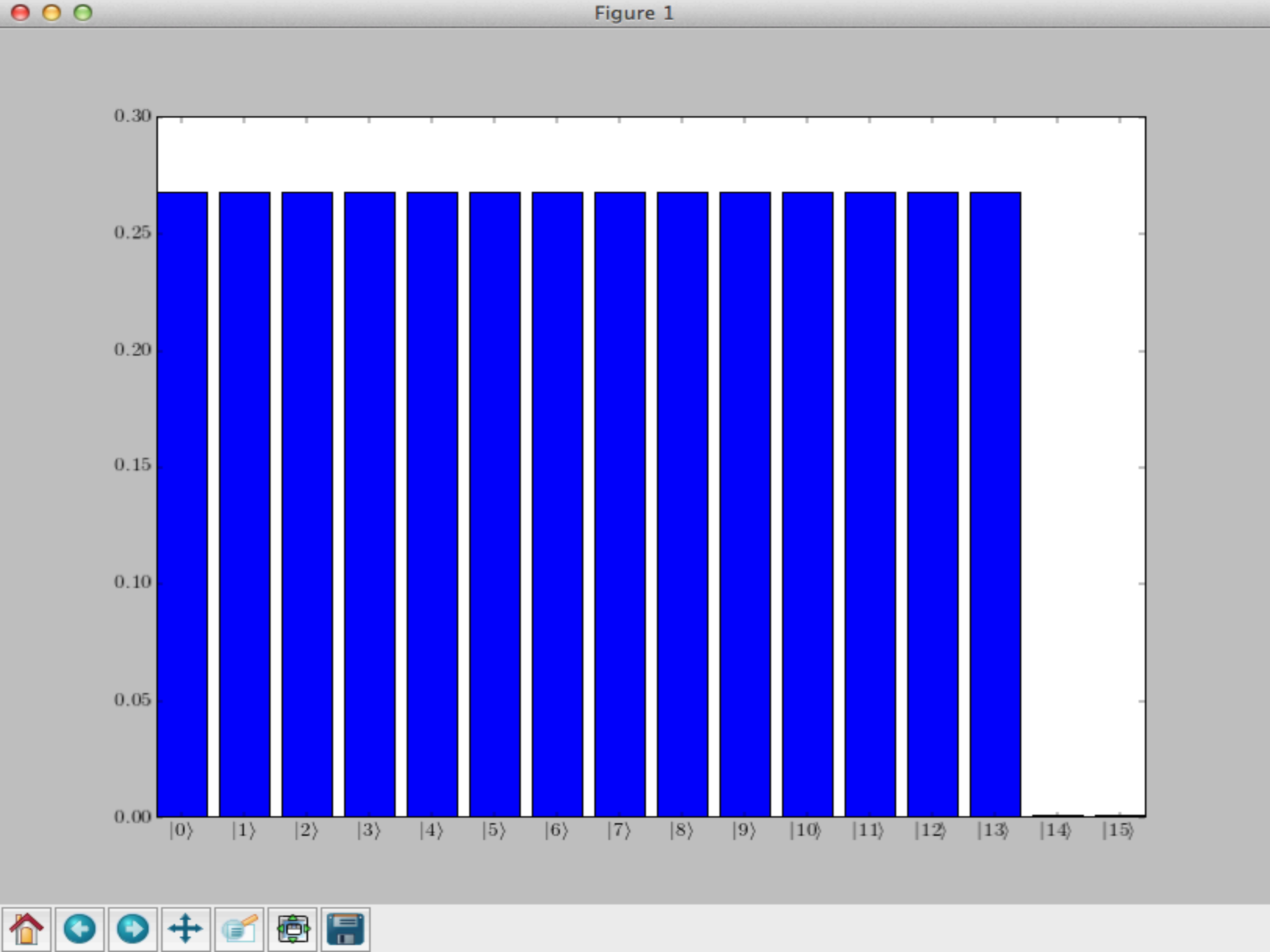
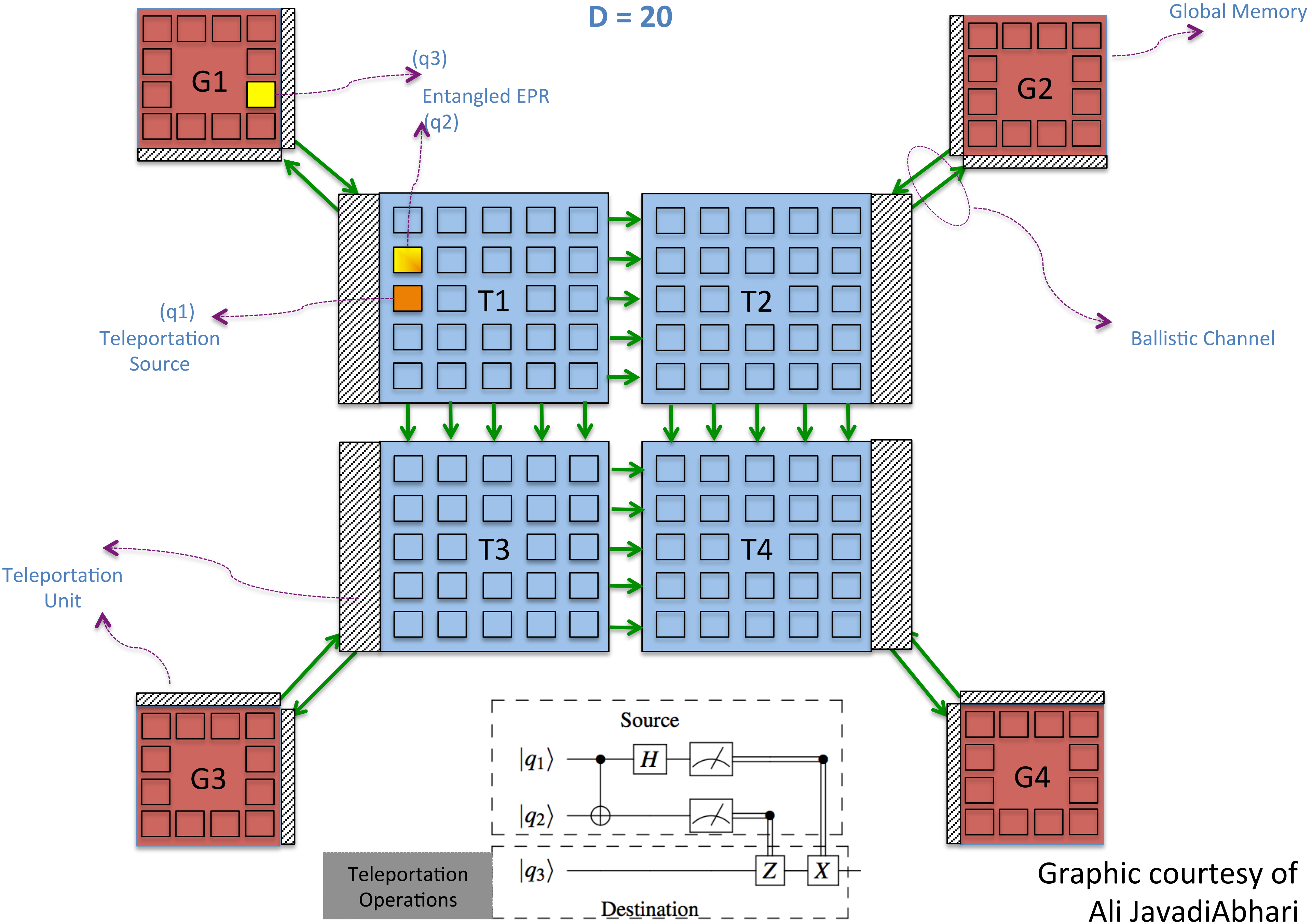


Figure 1
0.30
0.25
0.20
0.15
0.10
0.05
0.00
|0⟩
|1⟩
|2⟩
|3⟩
|4⟩
|5⟩
|6⟩
|7⟩
|8⟩
|9⟩
|10⟩
|11⟩
|12⟩
|13⟩
|14⟩
|15⟩

K = 4

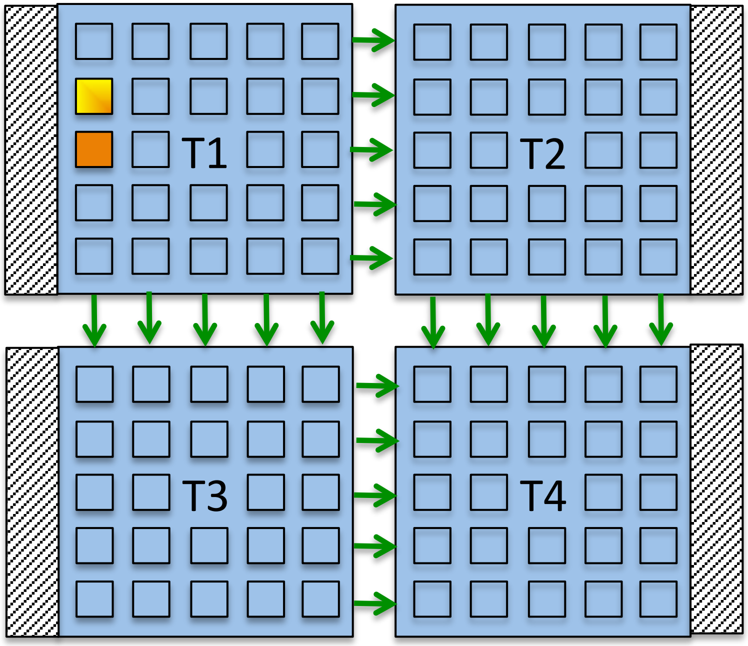
D = 20



Graphic courtesy of Ali JavadiAbhari

Scheduling Problem

- To move qubits, need entangled pairs ready at source and destination
- Could move all entangled pairs at start
- Could deliver entangled pairs "on demand"
- My project: find good tradeoff



Progress To Date

- Selecting new project
- Reading background papers
- Compiling code
  - New dev account
- Understanding code
- Playing around with priority queue approach

Progress To Date

- Selecting new project
- Reading background papers
- Compiling code
  - New dev account
- Understanding code
- Playing around with priority queue approach

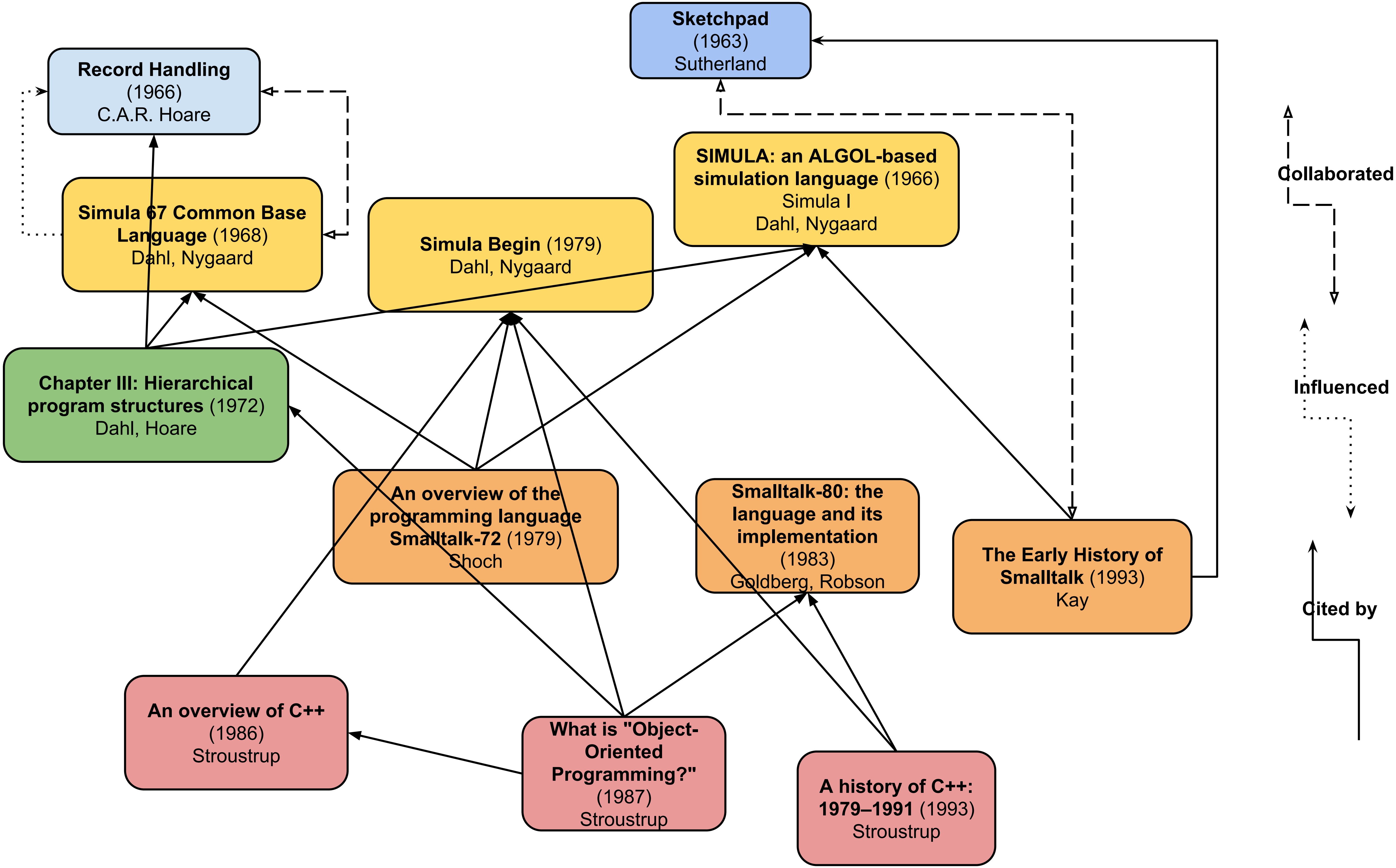
Next…

- Write a better smoothing algorithm
- Get results!

“Markerwitz”

by Dale Markowitz and Shubhro Saha

http://imgur.com/RJbB8Xs


Sketchpad (1963) Sutherland
Record Handling (1966) C.A.R. Hoare
SIMULA: an ALGOL-based simulation language (1966) Simula I Dahl, Nygaard
Simula 67 Common Base Language (1968) Dahl, Nygaard
Simula Begin (1979) Dahl, Nygaard
Chapter III: Hierarchical program structures (1972) Dahl, Hoare
An overview of the programming language Smalltalk-72 (1979) Shoch
Smalltalk-80: the language and its implementation (1983) Goldberg, Robson
The Early History of Smalltalk (1993) Kay
An overview of C++ (1986) Stroustrup
What is "Object-Oriented Programming?" (1987) Stroustrup
A history of C++: 1979–1991 (1993) Stroustrup
Collaborated
Influenced
Cited by

Boolean Algebra: Now and Then

Semih Yagli

Problems in Original Boolean Algebra

- x+y is well defined only if x and y are disjoint. ✗
- x-y is well defined only if x includes y as a subclass. ✗
- x^2=x is the Fundamental Law of Thought but x^3=x is meaningless! ✗

Some of my findings:

- Logical Algebra is introduced by Peirce (1867)
  - Logical addition: x+y is defined even when a and b are not mutually exclusive ✓
  - Logical multiplication: x.x.x.x.x.x.x.x.x=x ✓
  - Logical subtraction: x-y is still uninterpretable if y is not a subclass of x ✗
  - Logical division: Trying to keep duality of operations ✗
- J. Venn introduces Venn Diagrams (1881)
  - Boole did not have Venn diagrams !!!
  - Venn still cannot not resolve x-y issue. ✗

Some of my findings:

- Principia Mathematica re-defines symblic logic (1912)
  - «OR» and «AND» are analogous to logical addition and logical multiplication. ✓
  - Other logical operations are: «NOT», «IMPLIES» and «EQUIVALENCE». ✓
  - There is no counterpart of logical subtraction or logical division. ✓

To do:

- Project is mostly finished, spell check is required!
- If there are interested people, I can send them a copy of the latest draft.

Thank you for listening!

References:

[1] George Boole. An investigation of the Laws of Thought: on which are Founded the Mathematical Theories of Logic and Probabilities. Dover Publications, 1854.

[2] Charles S. Peirce. Five hundred and eightieth meeting. March 12, 1867. Adjourned statute meeting; on an improvement in Boole's calculus of logic. In Proceedings of the American Academy of Arts and Sciences, volume 7, pages 249-261, 1865.

[3] John Venn. Symbolic logic. Macmillan, 1881.

[4] Alfred North Whitehead and Bertrand Russell. Principia Mathematica, volume 1. University Press, 1912.

Enigma Simulator

COS 583

Thee Chanyaswad

What is the Enigma?

- An electro-mechanical enciphering/deciphering device used by the German during WWII.

PRINCETON UNIVERSITY

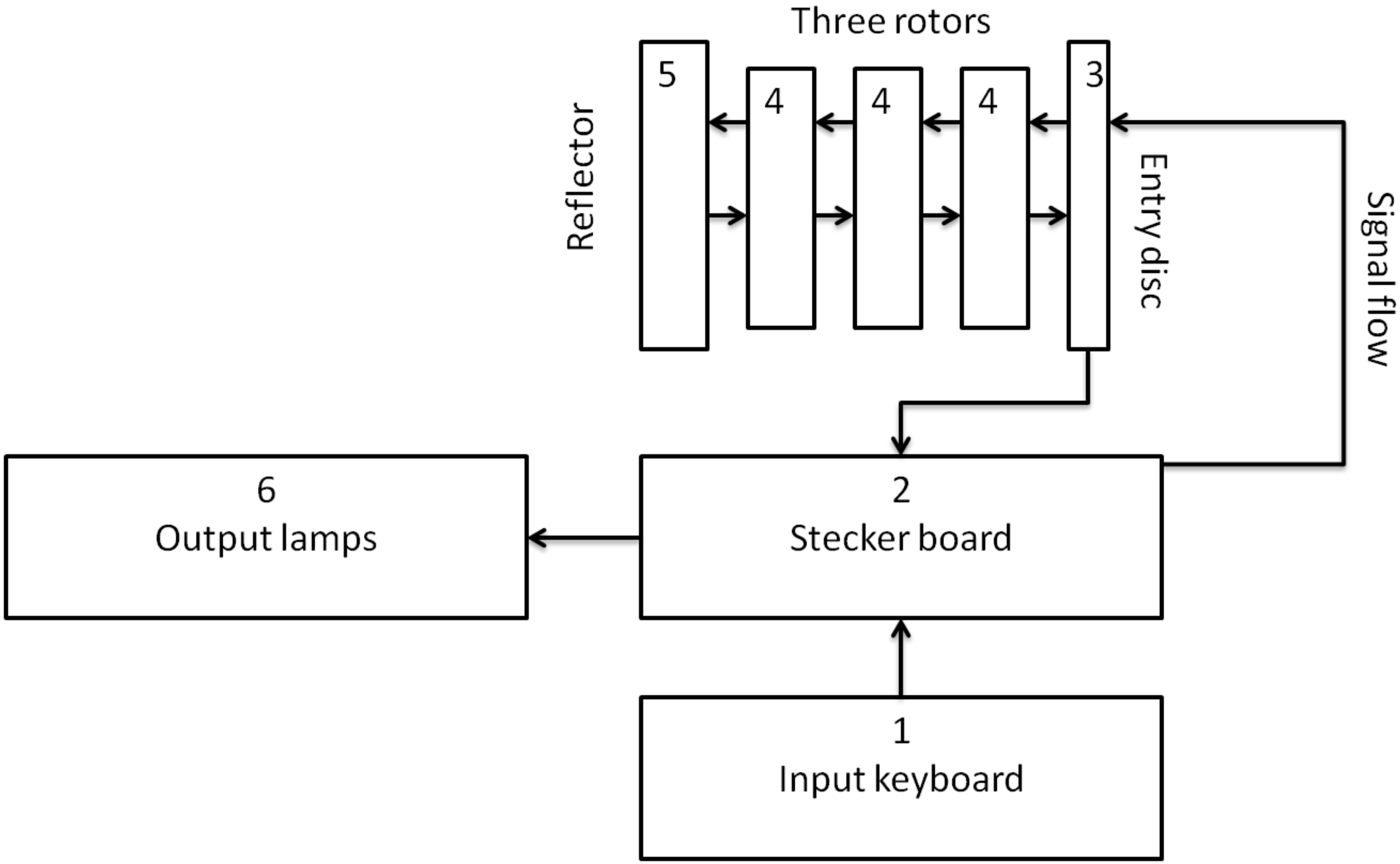
Image source: http://users.telenet.be/d.rijmenants/en/enigmatech.htm

Why is it important?

- The Enigma prompted Alan Turing and teams of code-breakers to develop machines to break it.
- Many of the team members went on to build the world's first generation of computers [1].

[1] http://www.cs4fn.org/history/colossus.php

The Enigma Basics



The Simulator

- Written in C++
- Done so far…
  - Created a class for each of the Enigma parts.
  - Finished the main operation function.
  - Wrote the majority of the display( ) function.
- To be finished…
  - The display( ) function.

THANK YOU.

Lightning Round

Themistoklis Melissaris

Project outline

- “From Weiser’s dream to the Cloud”
- Evolution of the field of ubiquitous computing
- Effects on ubiquitous computing by:
  - Hardware
  - Services
  - New concepts

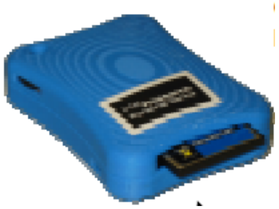
Papers

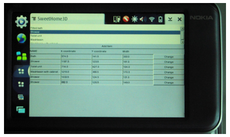
- Some Computer Science Issues in Ubiquitous computing, 1993
- Context-Aware Computing Applications, 1994
- People, Places, Things: Web Presence for the Real World, 2000
- The Personal Server: Changing the Way We Think about Ubiquitous Computing, 2002
- Calling the Cloud: Enabling Mobile Phones as Interfaces to Cloud Applications, 2009

Hardware/Concepts Timeline

Xerox PARC prototypes

PARCtab





Birth of UbiComp

Context-aware computing

Web Presence

Personal server

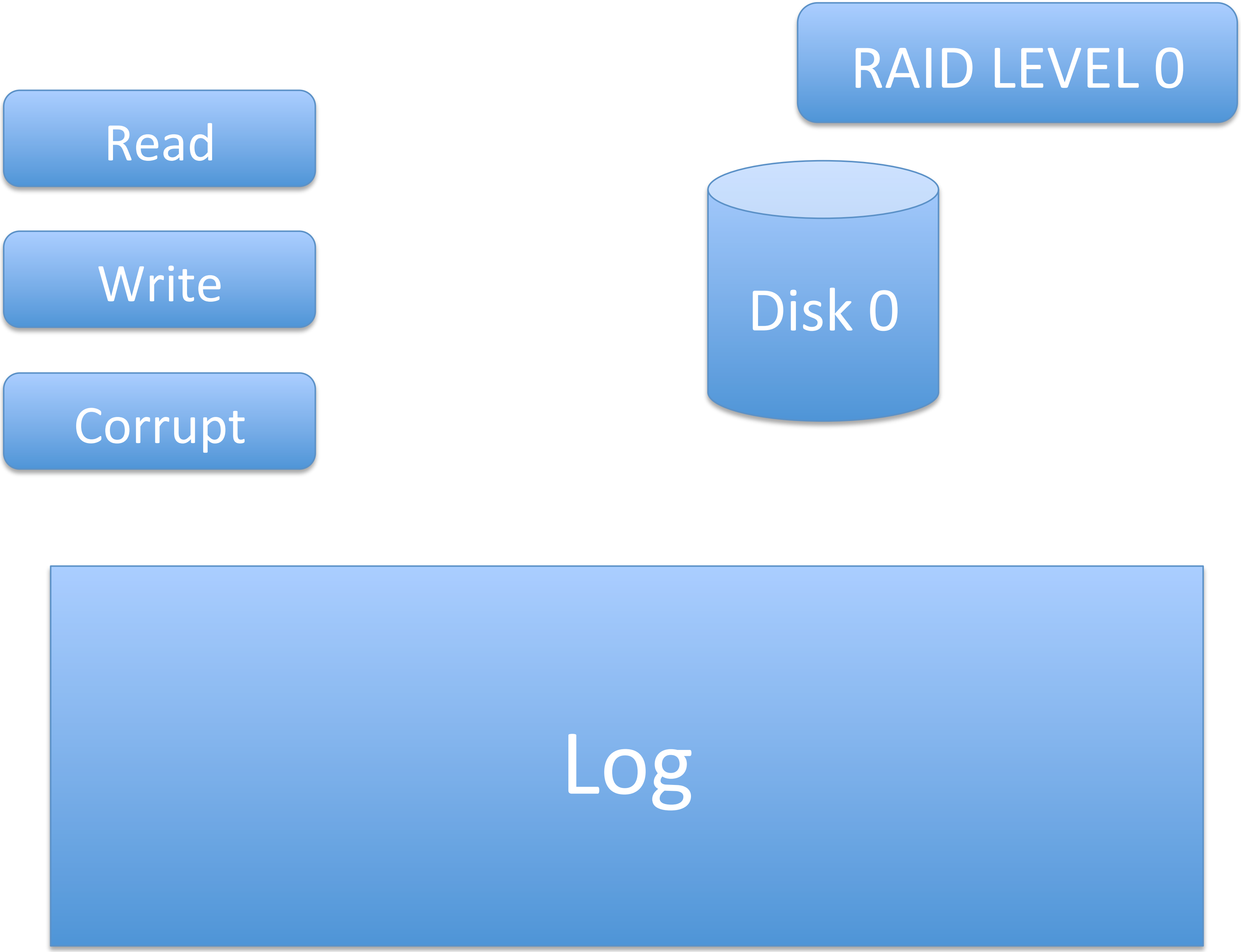
Computation offloading

To Do

- Are there any Weiser influences?
- Any predictions fulfilled?
- Citation chains and relationships
- My predictions

RAID Teaching Tool

By Utsarga Sikder



RAID LEVEL 0

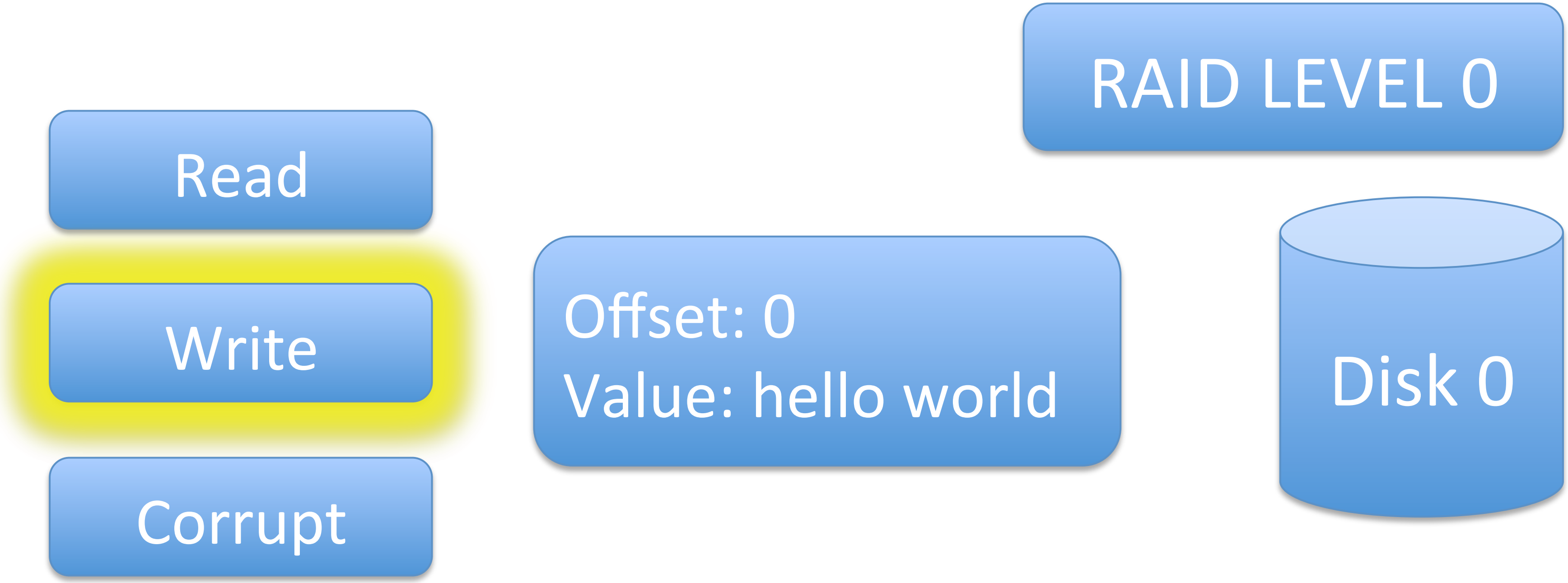
Read

Write

Corrupt

Disk 0

Log



RAID LEVEL 0

Read

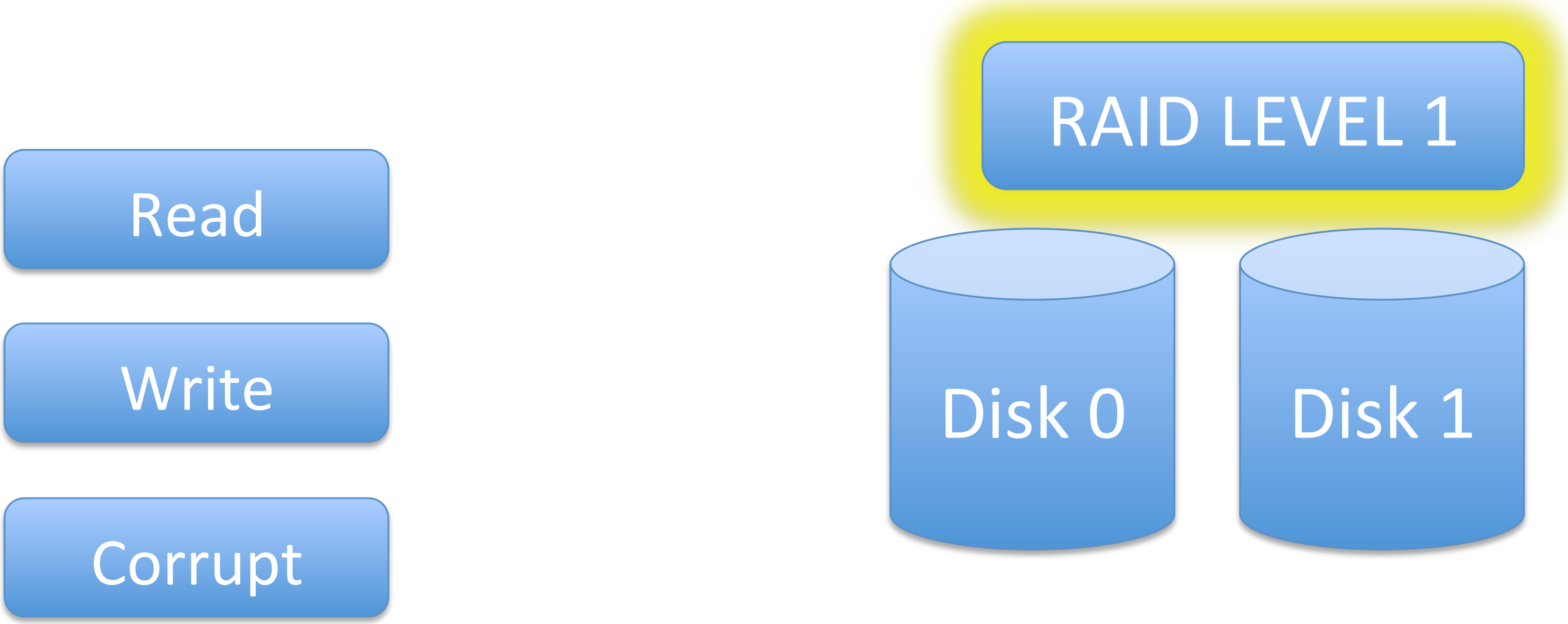
Write

Corrupt

Offset: 0
Value: hello world

Disk 0

Wrote “hello world” to disk 0, position 0.



Read

Write

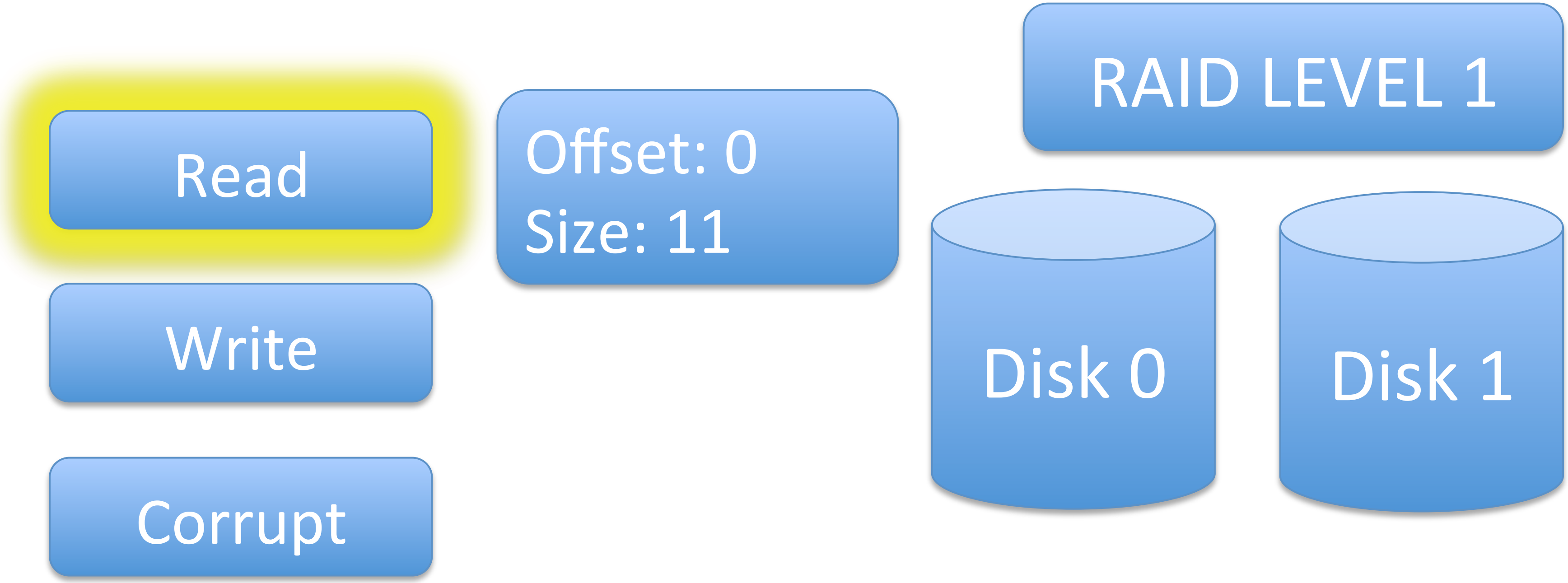
Corrupt

RAID LEVEL 1

Disk 0

Disk 1

Wrote data “hello world” to disk 0, position 0.
Switched to RAID L1.



Read

Write

Corrupt

Offset: 0

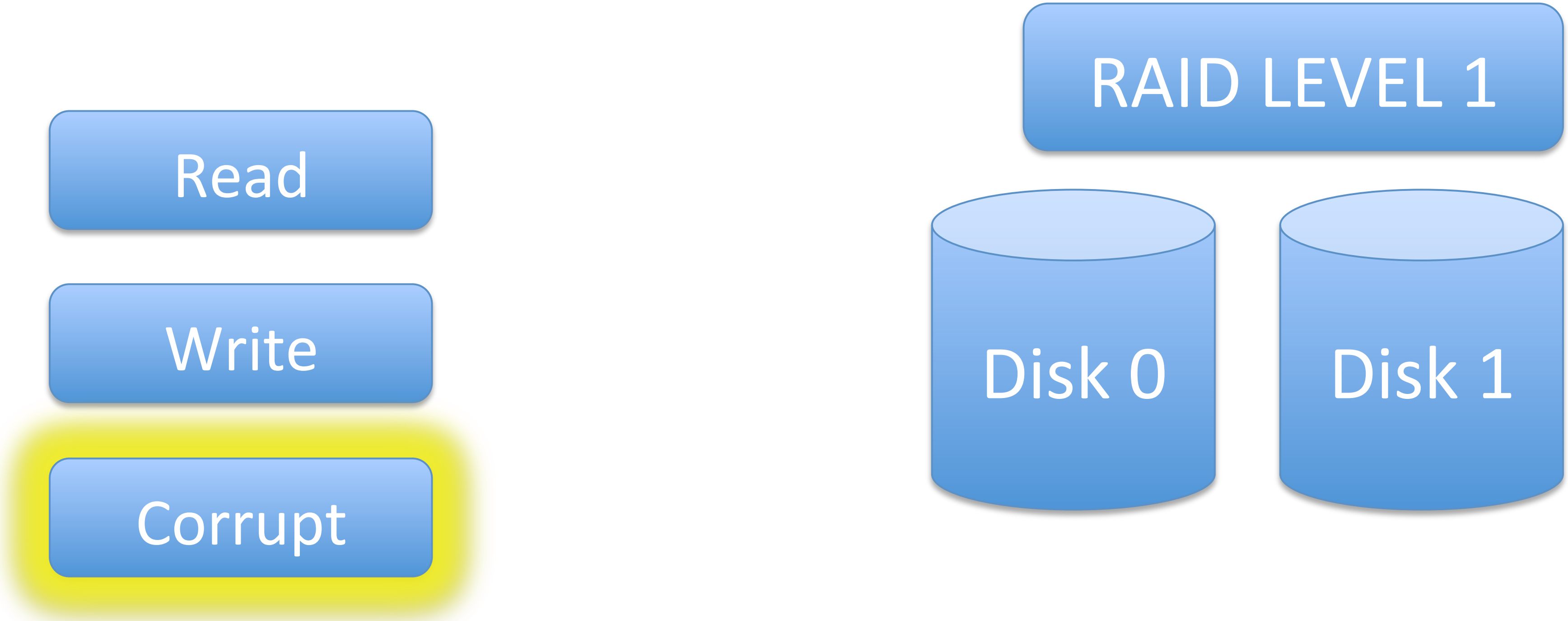
Size: 11

RAID LEVEL 1

Disk 0

Disk 1

Wrote “hello world” to disk 0, position 0.
Switched to RAID L1.
Read data “hello world” from d0, p0.
Read redundant data “hello world” from d1, p1.



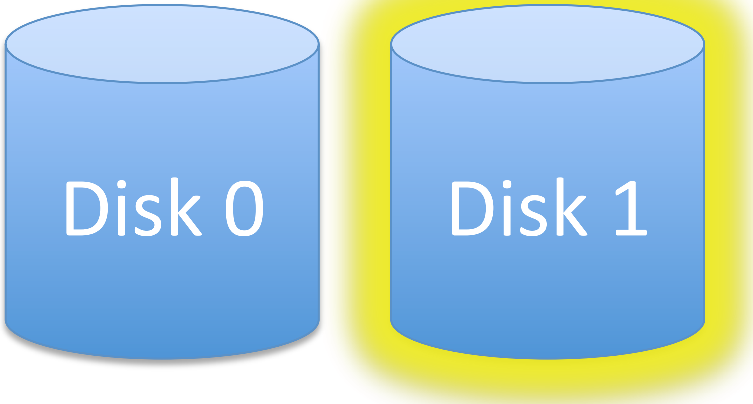
Switched to RAID L1.
Read data “hello world” from d0, p0.
Read redundant data “hello world” from d1, p1.
Corrupting disk 0. Recovered data using disk 1.

RAID LEVEL 1

Read

Write

Corrupt



Read data “hello world” from d0, p0.
Read redundant data “hello world” from d1, p1.
Corrupting disk 0. Recovered data using disk 1.
Dumping disk 1: “hello world ”

Tracing of data models of database

Nosql movement

- Michael Stonebraker ‘s talk at EPFL
- data warehouses will migrate to column-based data storeswithin 10 years. The traditional row-based data storage approach is dead, as row-based storage will never match column-based storage’s performance increase by factor 100x.
- the race for the best data storage designs has not yet been decided, but there is a clear indication of classic models being “plain wrong” (according to Stonebraker), as only 4% of wall-clock time is spent on useful data processing, while the rest is occupied with buffer pools, locking, latching, recovery.

Data Models Tracing

1970	Relational	A Relational Model of Data for Large Shared Data Banks
1976	Entity-relation	The Entity-Relationship Model - Toward a Unified View of Data
1981	semantic	Database Description with SDM: A Semantic Database Model
1983	Extended Relational	The Database Language GEM
1986	Object Oriented	An object server for an object-oriented database system
1986	Object Relational	The Design of Postgres
1997	Semi Structured	A Database Management System for Semi-structured Data
2006	Column Oriented	Bigtable: A Distributed Storage System for Structured Data

1970 A Relational Model of Data for Large Shared Data Banks

- **Relational database**
- Store the data in a simple data structure
- high level set-at-a-time DML
- No need for a physical storage proposal

1976 The Entity-Relationship Model - Toward a Unified View of Data

- **Entity relation**
- a collection of instances of entities
- entities have attributes
- there could be relationships between entities (1-to-1, 1-to-n, n-to-1 or m-to-n)
- Relationships can also have attributes

1981 Database Description with SDM: A Semantic Database Model

- **Semantic**
- relational data model is “semantically impoverished”, incapable of easily expressing a class of data of interest.
- “post relational” data model - Semantic data models
- focuses on the notion of classes, which are a collection of records obeying the same schema
- Have aggregation and generalization

1983 The Database Language GEM

- **Extended relational**
- Adding a new “feature” to the relational model to correct the problem
- proposed adding the following constructs to the relational model, together with corresponding query language extensions
  - set-valued attributes
  - aggregation

1986 An object server for an object-oriented database system

- Object-oriented
- an “impedance mismatch” between relational data bases and languages like C++
- to bind an application to the data base required a conversion from “programming language speak” to “data base speak” and back

1986 The Design of Postgres

- Object relational
- Motivated by GIS queries, which are difficult to express in SQL
- the OR proposal added
  - user-defined data types,
  - user-defined operators,
  - user-defined functions,
  - and user-defined access methods
- First prototype was Postgres

1997 A Database Management System for Semi-structured Data

- Semi- structured
  - Schema later
  - graph-oriented